

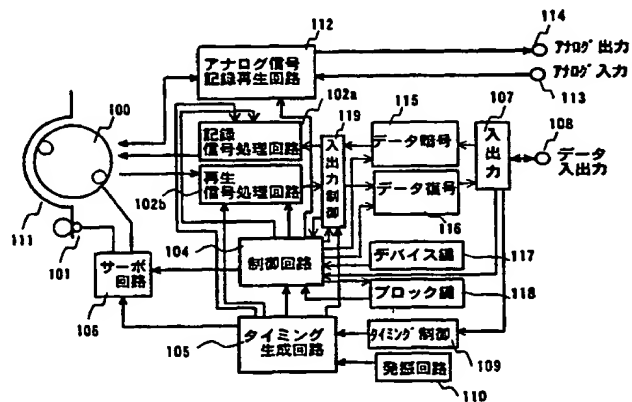
<p>(51) 国際特許分類6 G11B 20/10</p>	<p>A1</p>	<p>(11) 国際公開番号 WO00/52690</p> <p>(43) 国際公開日 2000年9月8日(08.09.00)</p>
<p>(21) 国際出願番号 PCT/JP99/00929</p> <p>(22) 国際出願日 1999年2月26日(26.02.99)</p> <p>(71) 出願人 (米国を除くすべての指定国について) 株式会社 日立製作所(HITACHI, LTD.)(JP/JP) 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo, (JP)</p> <p>(72) 発明者 ; および</p> <p>(75) 発明者 / 出願人 (米国についてのみ) 佐々本学(SASAMOTO, Manabu)(JP/JP) 相川 慎(AIKAWA, Makoto)(JP/JP) 岡本宏夫(OKAMOTO, Hiroo)(JP/JP) 野口敬治(NOGUCHI, Takaharu)(JP/JP) 〒244-0817 神奈川県横浜市戸塚区吉田町292番地 株式会社 日立製作所 マルチメディアシステム開発本部内 Kanagawa, (JP)</p> <p>(74) 代理人 弁理士 作田康夫(SAKUTA, Yasuo) 〒100-8220 東京都千代田区丸の内一丁目5番1号 株式会社 日立製作所内 Tokyo, (JP)</p>		<p>(81) 指定国 BR, CA, CN, IN, JP, KR, SG, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)</p> <p>添付公開書類 国際調査報告書</p>

(54)Title: DIGITAL SIGNAL RECORDER, REPRODUCER AND RECORDING MEDIUM

(54)発明の名称 デジタル信号記録装置、再生装置、および記録媒体

(57) Abstract

A recorder, a reproducer and a recording medium capable of protecting a copy right of a digital signal on a recording medium; specifically a digital signal recorder, a reproducer and a recording medium for recording or reproducing a digital signal onto or from a recording medium, wherein, at recording, a digital signal is encoded by a key obtained by performing a preset calculation on a key information and is recorded on a recording medium along with the key information, and at reproducing, a reproduced digital signal is decoded by the key reproduced from the recording medium and obtained by performing the preset calculation on the key information and is output.



- | | |
|---|------------------------------|
| 102a ... RECORDING SIGNAL PROCESSING CIRCUIT | 113 ... ANALOG INPUT |
| 102b ... REPRODUCING SIGNAL PROCESSING CIRCUIT | 114 ... ANALOG OUTPUT |
| 104 ... CONTROL CIRCUIT | 115 ... DATA ENCODING |
| 105 ... TIMING GENERATION CIRCUIT | 116 ... DATA DECODING |
| 106 ... SERVO CIRCUIT | 117 ... DEVICE KEY |
| 107 ... INPUT/OUTPUT | 118 ... BLOCK KEY |
| 108 ... DATA INPUT/OUTPUT | 119 ... INPUT/OUTPUT CONTROL |
| 109 ... TIMING CONTROL | |
| 110 ... OSCILLATION CIRCUIT | |
| 112 ... ANALOG SIGNAL RECORDING/REPRODUCING CIRCUIT | |

記録媒体上のデジタル信号の著作権を保護できる記録装置、再生装置、および記録媒体である。

デジタル信号を、記録媒体上に記録または再生するデジタル信号記録装置、再生装置、および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、デジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したデジタル信号を復号化して出力する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴ
BG	ブルガリア	GM	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア共和国	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサオ	ML	マリ	TT	トリニダード・トバゴ
CA	カナダ	HR	クロアチア	MN	モンゴル	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MR	モーリタニア	UA	ウクライナ
CG	コンゴ	ID	インドネシア	MW	マラウイ	UG	ウガンダ
CH	スイス	IE	アイルランド	MX	メキシコ	US	米国
CI	コートジボアール	IL	イスラエル	MZ	モザンビーク	UZ	ウズベキスタン
CM	カメルーン	IN	インド	NE	ニジェール	VN	ヴェトナム
CN	中国	IS	アイスランド	NL	オランダ	YU	ユーゴスラヴィア
CR	コスタ・リカ	IT	イタリア	NO	ノルウェー	ZA	南アフリカ共和国
CU	キューバ	JP	日本	NZ	ニュージーランド	ZW	ジンバブエ
CY	キプロス	KE	ケニア	PL	ポーランド		
CZ	チェッコ	KG	キルギスタン	PT	ポルトガル		
DE	ドイツ	KP	北朝鮮	RO	ルーマニア		
DK	デンマーク	KR	韓国				

明 細 書

ディジタル信号記録装置、再生装置、および記録媒体

技術分野

- 5 本発明は、ディジタル信号を記録媒体に記録再生するディジタル信号記録装置、再生装置、および記録媒体に関し、特に記録媒体上のディジタル信号の著作権を保護する機能を有する記録、再生装置、および記録媒体に関する。

背景技術

- 10 近年、ディジタル技術を用いた映像、音声等のデータ圧縮の研究が進み、これらデータの蓄積、伝送が容易にできるようになった。これに伴い、放送の分野においてもディジタル化が急速に進められている。

- 例えば、アナログ映像信号、音声信号をMPEG (Moving Picture Experts Group) 規格を用いて高能率にディジタル圧縮符号化し、衛星や
15 同軸ケーブルを通して放送するシステムが知られている。このディジタル放送を受信するための装置として、セットトップボックスと呼ばれるディジタル放送受信機がある。

- また、家庭用の映像信号、音声信号記録再生機器としては、磁気テープを用い、ディジタルTV放送などのディジタル圧縮符号化された映像
20 信号及び音声信号をディジタル信号のまま記録し再生できるディジタルVTRの開発が進められている。

このディジタル放送受信機とディジタルVTRは、ディジタルインターフェースで接続され、受信したディジタル放送を高品質で保存可能となる。

複数の情報が多重されて伝送されてくるデジタル信号を受信して所望の番組を選択する技術が、日本特開平 8 - 5 6 3 5 0 号に述べられている。また、回転磁気ヘッドを用いたデジタル V T R については、例えば、日本特開平 5 - 1 7 4 4 9 6 号に記載されている。

- 5 さらに、デジタル放送受信機とデジタル V T R をデジタルインターフェースで接続したデジタル放送記録システムについて、アイイーイーイー トランザクションズ オン コンシューマー エレクトロニクス、第 4 2 巻 3 号、1 9 9 6 年 8 月、6 1 7 ~ 6 2 2 頁 (IEEE Transactions on Consumer Electronics, Vol. 42, No. 3, August 1996, p617
10 ~ 622 「Newly Developed D-VHS Digital Tape Recording System for the Multimedia Era」) に詳しく述べられている。

しかしながら、デジタル放送等をデジタル V T R 等で記録した、
~~記録媒体上のデジタル信号の著作権の防衛については何ら考慮されて~~
いない。

- 15 本発明の目的は、記録媒体上のデジタル信号の著作権を保護することにある。

発明の開示

- 本発明は、デジタル信号を、記録媒体上に記録または再生するデ
20 ジタル信号記録装置、再生装置および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、デジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したデジタル信号を復号化して出力する。

25

図面の簡単な説明

第 1 図は本発明の実施例で、ディジタル放送受信機とディジタル信号記録再生装置を含む構成図である。

第 2 図は第 1 図のディジタル信号記録再生装置 2 0 0 の構成図である。

第 3 図はディジタル映像圧縮信号のパケットの構成図である。

5 第 4 図は第 3 図のパケットヘッダ 3 0 6 の構成図である。

第 5 図はディジタル放送の伝送信号及び伝送信号より選択された信号の構成図である。

第 6 図は第 2 図のデータ暗号回路 1 1 5 の構成図である。

第 7 図は第 6 図の暗号器 1 1 5 5 の構成図である。

10 第 8 図は第 2 図のデータ暗号回路 1 1 5、データ復号回路 1 1 6 に供給するデータ鍵の生成例を示すところの制御回路 1 0 4 内のデータ鍵の生成図である。

第 9 図はテープ 1 1 1 の 1 トラックの記録パターンを示す図である。

第 1 0 図は第 9 図のデータ記録領域 7 のブロックの構成図である。

15 第 1 1 図は第 1 0 図の I D 情報 2 1 の構成図である。

第 1 2 図は第 9 図のデータ記録領域 7 の 1 トラック分のデータの構成図である。

20 第 1 3 図は 1 8 8 バイトのパケット形式で伝送されたディジタル圧縮映像信号を、第 1 2 図のデータ 4 1 に記録する時の 1 パケットのブロックの構成図である。

第 1 4 図は第 1 2 図のデータ記録領域 7 のヘッダ 4 4 の構成図である。

第 1 5 図は第 1 4 図の付加情報 4 7 の領域に、ブロック鍵を格納する場合のバックデータの構成図である。

第 1 6 図はブロック鍵の格納方法を示す図である。

25 第 1 7 図はブロック鍵の他の格納方法を示す図である。

第 1 8 図は第 1 3 図の時間情報 2 5 の具体的構成図である。

第 19 図は第 2 図のデータ復号回路 116 の構成図である。

第 20 図は第 2 図の記録信号処理回路 102a および再生信号処理回路 102b からなるデジタル記録再生信号処理回路 102 の構成図である。

5 第 21 図はデータ記録開始時における信号処理のタイミングを示す図である。

第 22 図は第 2 図のテープ 111 上の鍵情報を示す図である。

第 23 図はデータ再生時における信号処理のタイミングを示す図である。

10 第 24 図は第 1 図のデジタル信号記録再生装置 200 の他の構成図である。

発明を実施するための最良の形態

以下、本発明の実施例を図面を用いて説明する。

15 第 1 図はデジタル放送受信機とデジタル信号記録再生装置を含む構成図である。200 はデジタル信号記録再生装置、201 はデジタル放送受信装置、202 はアンテナ、207 は受像機である。また、203 はチューナ、204 は選択回路、205 は復号回路、206 はインターフェース回路、208 はデジタル放送受信機 201 の動作の制
20 御を行う制御回路である。ここで、デジタル放送受信機 201 とデジタル信号記録再生装置 200 は別体の構成で表示されているが、一体の構成となってもよい。

第 2 図は第 1 図のデジタル信号記録再生装置 200 の構成図である。
図 2 は記録再生兼用の装置であるが、記録と再生が独立していても同様
25 である。100 は回転ヘッド、101 はキャプスタン、102a は記録時の記録信号の生成等を行う記録信号処理回路、102b は再生時の再

生信号の復調等を行う再生信号処理回路、104は記録再生モード等の制御を行う、例えば、マイクロプロセッサのような制御回路、105は回転ヘッド100の回転等の基準となるタイミング信号を生成するタイミング生成回路、106は回転ヘッド及びテープの送り速度を制御するサーボ回路、107は記録信号の入力または再生信号の出力を行う入出力回路、109は記録時のタイミングを制御するタイミング制御回路、110は基準クロックを生成する発振回路、111はテープ、112はアナログ映像信号の記録再生回路、115はデジタル信号記録時のデータ暗号回路、116はデジタル信号再生時のデータ復号回路、117は、デジタル情報を暗号あるいは復号する際にデータ暗号回路115あるいはデータ復号回路116に供給するデータ鍵のもとであるデバイス鍵を発生するデバイス鍵発生器、118はデジタル情報を暗号あるいは復号する際のデータ鍵のもう一つのもとであるブロック鍵を発生するブロック鍵発生器、119は記録時のパケットデータへのタイムスタンプ処理、再生時のパケットデータの出力制御を行う入出力制御回路である。

デジタル映像圧縮信号は、パケット形式のデータで、複数チャンネルの信号が時分割多重されて伝送される。図1において、アンテナ202で受信されたデジタル放送信号は、チューナ203で復調され、その後、選択回路204で必要なデジタル圧縮映像信号が選択される。選択されたデジタル圧縮映像信号は、復号回路205で通常の映像信号に復号されて、受像機207に出力される。また、受信信号にスクランブル等の処理が行われているときは、選択回路204においてそれを解除した後に、復号処理が行なわれる。受信したデジタル放送信号の記録を行うときは、選択回路204において記録するデジタル圧縮映像信号及びそれに関連した情報が選択され、インターフェース回路20

6を介してデジタル信号記録再生装置200の入出力端子108より、デジタル信号記録装置200に入力され、記録される。また、記録したデジタル放送信号の再生を行うときは、デジタル信号記録再生装置200で再生されたデジタル圧縮映像信号等が、入出力端子108よりインターフェース回路206に出力される。インターフェース回路206に入力されたデジタル圧縮映像信号等は、選択回路204、復号回路205により、通常の受信時と同様の処理を行って、受像機207に出力する。

第1図のデジタル信号記録再生装置200の構成を示す第2図において、記録時には、入出力端子108より入力されたパケットデータの一部が、入出力回路107を介して制御回路104に入力される。制御回路104では、パケットデータに付加されている情報あるいはパケットデータとは別に送られてきた情報によりパケットデータの種類等を検出し、検出結果によって記録モードを判断し、記録信号処理回路102a及びサーボ回路106の動作モードを設定する。次に入出力回路107は、記録するパケットデータをデータ暗号回路115に出力する。データ暗号回路115では、デバイス鍵発生器117およびブロック鍵発生器118により発生される鍵をもとに制御回路104において生成されるデータ鍵によって、入力されたパケットデータを暗号化し、これを入出力制御回路119に出力する。入出力制御回路119では、タイミング生成回路105からの時間情報をもとに、入力されたパケットデータにタイムスタンプを施し、これを記録信号処理回路102aに出力する。記録信号処理回路102aでは、制御回路104で判断された記録モードに応じて、誤り訂正符号、ID情報、サブコード、暗号化に使用したブロック鍵情報等を含む記録データの生成を行い且つ記録信号を生成して、回転ヘッド100によりテープ111に記録する。

再生時には、まず任意の再生モードで再生動作を行い、再生信号処理回路 1 0 2 b で I D 情報を検出する。そして、制御回路 1 0 4 でどのモードで記録されたかを判断し、再生信号処理回路 1 0 2 b 及びサーボ回路 1 0 6 の動作モードを再設定して再生を行う。再生信号処理回路 1 0 2 b では、回転ヘッド 1 0 0 より再生された再生信号より、同期信号の検出、誤り検出訂正、ブロック鍵情報等の取得を行い、パケットデータを再生して入出力制御回路 1 1 9 に出力する。入出力制御回路 1 1 9 では、タイミング生成回路 1 0 5 で生成されたタイミングを基準としてタイムスタンプを取り除いたパケットデータをデータ復号回路 1 1 6 に出力する。データ復号回路 1 1 6 では、デバイス鍵発生器 1 1 7 により発生される鍵、および再生によって得られたブロック鍵をもとに、制御回路 1 0 4 において生成されるデータ鍵によって復号して、入出力回路 1 0 7 に出力する。

記録時には、入出力端子 1 0 8 より入力された記録データのレートを基準としてタイミング制御回路 1 0 9 により記録再生装置の動作タイミングを制御し、再生時には、発振回路 1 1 0 により発振されたクロックを動作基準として動作する。

第 3 図はディジタル映像圧縮信号のパケットの構成図である。1 パケットは固定長、例えば、1 8 8 バイトで構成されており、4 バイトのパケットヘッダ 3 0 6 と、1 8 4 バイトのパケット情報 3 0 7 により構成されている。ディジタル圧縮映像信号は、パケット情報 3 0 7 の領域に配置される。また、パケットヘッダ 3 0 7 はパケット情報の種類等の情報により構成される。

第 4 図は第 3 図のパケットヘッダ 3 0 6 の構成図である。5 0 1 はパケットの先頭を示す同期バイト、5 0 2 は誤りの有無を示す誤り表示、5 0 3 はユニットの開始を示すユニット開始表示、5 0 4 はパケットの

重要度を示すパケットプライオリティ、505はパケットの種類を示すパケットID、506はスクランブルの有無を示すスクランブル制御、507は追加情報の有無及びパケット情報の有無を示すアダプテーションフィールド制御、508はパケット単位でカウントアップされる巡回カウンタである。

第5図はディジタル放送の伝送信号及び伝送信号より選択された信号の構成図である。71は図3のパケットである。通常、上記映像信号に音声信号、プログラムに関する情報等が付加され、複数チャンネルのプログラムが時分割多重されて伝送される。

10 第5図(a)は、3チャンネルのプログラムを多重した例であり、V1、V2、V3はそれぞれのチャンネルの映像信号、A1、A2、A3はそれぞれのチャンネルの音声信号のパケットである。なお、映像または音声は、一つのチャンネルに複数の映像または音声で構成されている場合もある。P0、P1、P2、P3はプログラムに関する情報である。

15 それぞれのパケットは、異なるパケットID505が割り当てられており、これによりパケットの内容を識別することができる。

P0は、第5図(a)の伝送信号全体に関する情報であり、それぞれのプログラムにどのパケットIDが割り当てられているかを認識するためのプログラムアソシエーションテーブル、番組ガイド情報等のパケットが時分割多重されて伝送される。P1、P2、P3は、それぞれのプログラムに関する情報であり、そのチャンネルの映像パケット、音声パケット等にどのパケットIDが割り当てられているかを認識するためのプログラムマップテーブル、スクランブル情報等のパケットが時分割多重されて伝送される。通常、プログラムアソシエーションテーブルのパ

20

25

ケットIDは決まった値、例えば0が割り当てられている。

受信時には、まずプログラムアソシエーションテーブルによって受信

したいプログラムのプログラムマップテーブルにどのパケットIDが割り当てられているかを認識し、次に、受信したいプログラムのプログラムマップテーブルによって映像パケット、音声パケット等にどのパケットIDが割り当てられているかを認識する。そして、映像パケットおよび音声パケットを抽出してディジタル圧縮データの復号を行う。また、同時にプログラムクロックリファレンスを抽出し、これによってディジタル圧縮データの復号回路の復号タイミングが符号化時のタイミングと同期するように復号回路の動作を制御する。

CRは、ディジタル圧縮データの復号時の同期をとるためのプログラムクロックリファレンス情報である。

もちろん、多重するチャンネル数は3チャンネル以外、例えば4チャンネルでもよいし、また、これ以外の情報を多重してもよい。

第5図(b)は、第5図(a)から第1のチャンネルの情報およびそれに関連したプログラム情報のみを選択したものである。第1のチャンネルを記録する場合には、この情報をディジタル放送受信機201から記録再生装置200に出力する。もちろん、これ以外の情報を含めて記録してもよいし、また、再生時の処理をやりやすくするために、パケットの情報の一部を変更してもよい。例えば、プログラムアソシエーションテーブルの情報を記録するプログラムのみの情報に変更すれば、再生時にチャンネルの選択が不要になる。

第6図は第2図のデータ暗号回路115の構成図である。1151はパケットデータ入力端子、1157はパケットデータ出力端子、1153a、1153bはデータ鍵入力端子、1153cはデータ鍵選択信号入力端子、1153dは、処理モード選択信号入力端子、1152、1156はブロック処理回路、1154は鍵スケジュール回路、1155は暗号器、1158a、1158bはデータ鍵レジスタ、1159はデー

データ鍵セクタである。データ暗号回路 115 は、あらかじめ定められたデータ鍵により、入力されるパケットデータ単位で暗号化して出力する。この際、このデータ鍵をある時間間隔で変更していくことにより、テープ上に記録されるパケットデータの安全性を高めることができる。

- 5 暗号器 1155 は、例えば、伝送中にビット誤り等のエラーが発生しても、そのエラーが後続のデータに影響を与えない、すなわちエラー伝播がないように、複数ビットで構成されるブロックを単位として暗号処理を簡単な回路構成で実現できるブロック暗号を用いる。

- 10 入力端子 1151 から入力されたパケットデータは、まず、ブロック処理回路 1152 において、複数ビットからなるブロック P に区切られる。例えば 1 ブロックを 64 ビットとする。各ブロックは、暗号器 1155 において順次暗号化され、その結果ブロック C を出力し、ブロック

- ~~処理回路 1156 において、今度はブロックをパケットデータの形式に~~
戻して出力端子 1157 へ出力する。ここで、暗号化のための鍵である
15 データ鍵は、制御回路 104 より、データ鍵入力端子 1153a および 1153b から入力され、データ鍵レジスタ 1158a、1158b に記憶される。例えば、データ鍵レジスタ 1158a には、現在のデータ鍵を、データ鍵レジスタ 1158b には次に切り換えるデータ鍵を記録させる。

- 20 また、データ鍵選択信号入力端子 1153c からは、制御回路 104 より、データ鍵レジスタ 1158a、1158b のどちらのデータ鍵を選択するかを示す信号が入力され、データ鍵セクタ 1159 により、選択されたデータ鍵が出力される。ここでは、例えば鍵レジスタ 1158a のデータ鍵が選択されているものとする。選択されたデータ鍵は、
25 スケジュール回路 1154 においてサブ鍵 KA、KB に変換され、暗号器 1155 に供給される。例えば、データ鍵の長さ 56 ビット、サブ鍵

の長さが、それぞれ32ビットとし、データ鍵の上位32ビットをKAに割り当て、データ鍵の上位32ビットと下位32ビットの加算値をKBに割り当てる。

ここで、データ鍵を変更する場合には、制御回路104より、データ
5 鍵レジスタ1158bを出力するようデータ鍵選択信号入力端子1153cから信号が入力される。データ鍵セレクトは、一つのブロックデータのブロック全ての暗号化が終了するまでは、その選択出力を切り換えず、次のブロックデータとの間で切り換えるよう制御する。

その他、例えば、暗号器1155の出力と、暗号器1155の入力を
10 排他的論理和をとり、ブロック単位でフィードバックをかけることで、暗号強度を増す方法もある。

第7図は第6図の暗号器1155の構成図である。同図中、551、
552、553、554は暗号処理部、Pa、Pbは入力ブロックデータPの上位および下位ビット、Ca、Cbは暗号化されたデータ、KA、
15 KBは、サブ鍵である。同図に示すように、例えば入力された64ビットのブロックPを、その上位32ビットPaと下位32ビットPbに分離する。そのPa、Pbは、暗号処理部551において、排他的論理和(5511)、ビットシフトおよび加算演算(5512、5513、5515 : $A \ll p$ は、Aをpビット左方向に循環ビットシフトすることを表す)、加算演算(5514、5516)を行い、その結果を暗号
20 処理部551と同様の処理を行う後続の暗号処理部552、553、さらに図示しない暗号処理部に入力して複数段繰り返し演算を行い、最終段の暗号処理部554により出力されたデータCa、Cbより、暗号化されたブロックCを得る。

25 以上は、第2図、第7図のデータ暗号回路115について説明したが、第2図のデータ復号回路116では、暗号器1155の逆の流れで演算

していくことにより、暗号化されたブロックを復号することができる。
ただし、第7図の演算5516は、減算処理とする。また、当然、サブ
鍵KA、KBは、暗号時と同一の鍵を用いなければならない。

その他、記録するパケットデータを保護する必要が無い場合、例えば
5 記録する番組が自由にコピーしてもよいよう許可されている場合、パケ
ットデータを暗号化しないで、そのままテープ上に記録する場合がある。
これは例えば、データ暗号回路115、データ復号回路116を、入力
パケットの暗号・復号の機能と、なにもしないで通過させる機能とを切り
り換えることで実現できる。第2図、第6図のデータ暗号回路115に
10 おいて、第6図の処理モード選択信号入力端子1153dを介して入力
される処理モード選択信号により、第7図の演算5516への入力X5
を、図示していないが、零に固定することで、暗号、復号処理を行わず
~~に、ブロックを通過させることが出来る。この方法によれば、入力パケ~~
ットの通過遅延時間を一定に保ったまま、動作を切り換えることができ
15 る。また、図示しないが、他の方法としては、入力端子1151から入
力されたパケットデータを、ブロック処理回路1152、暗号器115
5、ブロック処理回路1156を介さず、出力端子1157に出力する
か、ブロック処理回路1156から出力されるパケットデータを出力端
子1157に出力するかを切り換える切り換え回路を出力端子1157
20 の前段に設け、処理モード選択信号入力端子1153dを介して入力さ
れる処理モード選択信号をその切り換え回路に入力して、ブロック処理
回路1156から出力されるパケットデータか、入力端子1157に入
力されたパケットデータかを切り換える方法もある。これらの方法は、
第2図、第19図のデータ復号回路116においても前述と同様の構成
25 で実現できる。

第8図は第2図のデータ暗号回路115、データ復号回路116に供

給するデータ鍵の生成例を示すところの制御回路104内のデータ鍵の生成図である。デバイス鍵発生器117は、例えば96ビットのあらかじめ定められた固定の鍵情報を記憶している。ブロック鍵発生器118は、例えば第2図の制御回路104からの司令1181により、96ビットの乱数を発生させる乱数発生器である。120は96ビットの排他的論理和演算器、121はハッシュ関数演算器である。第8図(a)では、ブロック鍵とデバイス鍵は、排他的論理和演算器120で排他的論理和がとられ、ハッシュ関数演算器121にてハッシュ演算がなされ、その結果のうちの選択された56ビットが、データ鍵として第2図のデータ暗号回路115に供給される。ハッシュ関数は、その出力結果から、入力データが類推困難な関数であり、データ鍵から、秘密情報であるブロック鍵、デバイス鍵が求められない。

また、第2図の制御回路104からの司令1181をある時間間隔で発生させ、上述の演算によるデータ鍵生成を繰り返し行うことにより、データ鍵を順次変更していくことができ、記録媒体上のデータの安全性を高めることが可能となる。次に、ブロック鍵発生器118で発生されたブロック鍵(K_r)は、第2図の記録信号処理回路102aに送られ、テープ111上に記録される。

再生時には、ブロック鍵発生器118の発生するブロック鍵の代わりに、テープ111上から再生されたブロック鍵(K_p)を用いて、上記と同様の演算を行い、データ鍵を得、第2図のデータ復号回路116に供給される。

第8図(b)は、テープ111上に記録する鍵情報K_rとして、ブロック鍵をデバイス鍵で排他的論理和演算したものをを用いる例である。この場合、ハッシュ関数演算器にはブロック鍵そのものが入力される。再生時には、第8図(a)中のブロック鍵の代わりに、テープ111上か

ら再生された K_p を用いて、上記と同様の演算を行い、データ鍵を得、データ復号回路 116 に供給される。

次に、テープへの記録方法について述べる。

図 9 は、1トラックの記録パターンである。3 は時間情報、プログラム情報等のサブコードを記録するサブコード記録領域、7 はデジタル圧縮映像信号を記録するデータ記録領域、2 及び 6 はそれぞれの記録領域のプリアンプル、4 及び 8 はそれぞれの記録領域のポストアンプル、5 はそれぞれの記録領域の間のギャップ、1 及び 9 はトラック端のマージンである。このように、各記録領域にポストアンプル、プリアンプル及びギャップを設けておくことにより、それぞれの領域を独立にアフレコを行うことができる。もちろん、記録領域 7 にはデジタル圧縮映像信号以外のデジタル信号を記録してもよい。データ記録領域 7 は、複数のブロック（前述の暗号化の小単位であるブロックとは異なる）により構成されている。

第 10 図は第 9 図のデータ記録領域 7 のブロックの構成図である。20 は同期信号、21 は ID 情報、22 はデータ、23 は第 1 の誤り検出訂正のためのパリティ（C1 パリティ）である。例えば、同期信号 20 は 2 バイト、ID 情報 21 は 3 バイト、データ 22 は 99 バイト、パリティ 23 は 8 バイトで構成されており、1 ブロックは 112 バイトで構成されている。

第 11 図は第 10 図の ID 情報 21 の構成図である。31 はグループ番号、32 はトラックアドレス、33 は 1 トラック内のブロックアドレス、35 はグループ番号 31、トラックアドレス 32 及びブロックアドレス 33 の誤りを検出するためのパリティである。ブロックアドレス 33 は、各記録領域でのブロックの識別を行うためのアドレスである。例えば、第 9 図のデータ記録領域 7 では 0 ～ 335 とする。トラックアド

レス 3 2 は、トラックの識別を行うためのアドレスであり、例えば、1
トラックまたは2トラック単位でアドレスを変化させ、nトラックを識
別することが出来る。例えば、0～5または0～2とすることにより、
6トラックを識別することができる。第11図のグループ番号31は、
5 例えば、トラックアドレス32で識別する6トラック単位で変化させ、
0～15とすることにより、96トラックを識別することができる。ト
ラックアドレス32は、後述する第2の誤り訂正符号の周期と同期させ
ておけば、記録時の処理及び再生時の識別を容易にすることができる。

第12図は第9図のデータ記録領域7の1トラック分のデータの構成
10 図である。なお、第10図に図示の同期信号20およびID情報21は
省略してある。データ記録領域7は、例えば、336ブロックで構成さ
れており、最初の306ブロックにデータ41を、次の30ブロックに
第2の誤り訂正符号(C2パリティ)43を記録する。C2パリティ4
3は、nトラック単位、例えば6トラック単位で構成されている。6ト
15 ラック単位でみると、データは306ブロック×6トラックのデータで
あり、そのデータを18分割して、それぞれの102ブロックに、10
ブロックのC2パリティを付加する。誤り訂正符号は、例えばリードソ
ロモン符号を用いればよい。各ブロック99バイトのデータは、3バイ
トのヘッダ44と96バイトのデータ41により構成されている。

20 第13図は、188バイトのパケット形式で伝送されたデジタル圧
縮映像信号を、第12図のデータ41に記録する時の1パケットのブロ
ックの構成例である。この場合には、4バイトの時間情報25を付加し
て192バイトとし、2ブロックに1パケットを記録する。時間情報2
5は、パケットの伝送された時間の情報である。すなわち、パケットの
25 先頭が伝送された時の時間またはパケット間の間隔を基準クロックでカ
ウントし、そのカウント値をパケットデータと共に記録しておき、再生

時にその情報を基にしてパケット間の間隔を設定することにより、伝送された時と同一の形でデータを出力することができる。

第14図は第12図のデータ記録領域7のヘッダ44の構成図である。ヘッダ44は、フォーマット情報45、ブロック情報46および付加情報47により構成される。フォーマット情報45、およびブロック情報46には、記録に関する様々な記録情報が、また付加情報47には、その他補助的な情報が記録される。

フォーマット情報45は、記録フォーマットに関する情報であり、記録モード（標準速モードその他の識別）、取り扱うパケットデータの種類、記録されているパケットデータがコピー可能か否か等を示すコピー制限情報等が格納され、複数のブロックで、1つの情報を構成する。例えば12ブロックの12バイトで1つの情報を構成している。そして、この情報を複数回繰り返し返し多重記録することにより、再生時の検出能力を向上させている。ここに、前述の鍵情報等をも記録しておくことが可能である。

ブロック情報46は、データ記録領域41に記録されるデータの種別を識別するための情報である。ここには、高速可変速再生用データの有無、種類（どの速度に対応した高速可変速再生用データであるか）等を記録しておく。ここに、前述の鍵情報等をも記録しておくことも可能である。

付加情報47は、例えば、6ブロックの6バイトで一つの情報であるパックデータを構成し、最初の1バイトが情報の種類を表すアイテムコード、残りの5バイトをデータとすることにより、いろいろな種類のデータを記録することができる。例えばここに前述のブロック鍵等の鍵情報や、その他、記録時間等の情報や記録信号の種類等を記録しておくことができる。

第15図は第14図の付加情報47の領域に、ブロック鍵を格納する場合のパックデータの構成図である。

パックデータの最初の1バイトには後続の情報が鍵情報であることを示すアイテム情報コードを格納する。

- 5 2バイト目には、格納されている鍵の種類を示す情報（鍵シーケンス番号、鍵属性、鍵フラグ）を記録する。前述のように、ブロック鍵をある時間間隔で順次変更していくことで、記録媒体上のデータの安全性を高めることができるので、例えば、このパックに格納されているブロック鍵が、現在のパケットデータの暗号化に用いられるブロック鍵か、次に用いるブロック鍵かを示す鍵属性情報を記録しておく。また、ブロック鍵が更新される度に反転する鍵フラグで、切り換えタイミングを記録する。この情報により再生時の鍵の切り換えをスムーズにする。また、鍵シーケンス番号には、一つのパックでブロック鍵が格納できない場合、後続のパックがあることを示す情報を格納する。例えばブロック鍵が9
10 6ビットの場合、3つのパックに分割して格納し、それぞれの鍵シーケンス番号には、2、1、0を格納し、0が最終パックであることを示す。その他、全体のデータのサイズを格納しておき、残りの大きさを知る方法もある。

3バイト目から6バイト目に、ブロック鍵を収納する。

- 20 前述の第8図（b）の例では、鍵情報K_rがブロック鍵の代わりに格納される。

- 第16図はブロック鍵の格納方法を示す図である。この例は、各トラックのパックデータには、現在の鍵情報のみを記録する場合である。したがって、前述の鍵属性は、現在の鍵を示すのみの固定情報であり、記録しなくてもよい。同図中（1）は、96ビットの現在のブロック鍵A（A₀乃至A₁₁）が3個のパックに分割して格納される状態を示す。
- 25

通常、これらのパックは、データの信頼性の向上のため、一つのトラックにつき、複数回記録される。例えば、3個のパックをトラックの最初、半ば、最後のそれぞれの領域に記録する（計9個）ことで、磁気ヘッドの目詰まり等による、再生信号のバースト欠落の影響を軽減できる。また、3個のパックは必ずしも連続したパックとして記録する必要はなく、各パックの間に他の情報を格納したパックを挿入し、鍵情報を格納しているパックを分散して記録することで、鍵情報自身の保護も可能となり、さらに信頼性が向上する。同図（2）はブロック鍵がBに切り換わったトラックに記録されるパックデータである。この場合、ブロック鍵Bの鍵フラグは反転している。

第17図はブロック鍵の他の格納方法を示す図である。第17図は、現在の鍵情報と共に、次に使用する鍵情報もあらかじめ発生させておき記録する方法である。ここで、鍵属性情報は、現在のパケットデータの暗号化に用いられるブロック鍵の場合“0”、次に用いるブロック鍵の場合“1”とする。また、ブロック鍵が更新される度に反転する鍵フラグは“0”と“1”を交互に繰り返す。

同図中（1）は、96ビットの現在のブロック鍵Aが格納される状態を示す。（2）には、次のブロック鍵Bが格納される。この（1）および（2）が、同一のトラック内のブロックの付加情報エリアに記録される。（3）は、ブロック鍵がBに切り換わったトラックに記録されるパックデータである。この場合、ブロック鍵Bは、鍵属性情報“0”の現在の鍵に、また、鍵フラグも反転している。さらに（4）は、次に用いる鍵Cが格納される。（3）および（4）が、同一のトラック内のパックデータとしてトラックに記録される。

ブロック鍵の更新タイミングを示す鍵フラグの格納場所としては、付加情報47のパックに格納する以外に、前述の第14図に示したフォー

マット情報 45、あるいはブロック情報 46 に格納する方法もある。

以上のように、鍵情報が、テープ上に記録されるが、ブロック鍵を切り換えるタイミングとしては、前述の C2 パリティの付加の単位である n トラック（本実施例では 6 トラック）の区切り目とすることで、再生時に、C2 パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

また、以上の例ではブロック鍵が更新されるタイミングを示す情報を鍵フラグとして記録したが、第 2 図の記録信号処理回路 102a において、前述の第 1 図に示したトラックアドレス 32、あるいはグループ番号 31 の値と、C2 パリティの演算の周期および更新のタイミングを同期させることで、特に鍵フラグを記録しなくとも、再生時における鍵情報の更新のタイミングを、このトラックアドレス 32 あるいはグループ番号 31 の値で検出することも可能である。例えば、第 2 図の記録信号処理回路 102a において、トラックアドレス 32 が、トラック 1 本毎に 0 から 5 の値を繰り返し、その値 0 から 5 の 6 本のトラックを、前述の C2 パリティの付加の単位とする。そして、値が 5 から 0 になるタイミングで、データ暗号回路 115 において、ブロック鍵を更新して、記録する。再生時においては、第 2 図の再生信号処理回路 102b において、このトラックアドレス 32 の値が 5 から 0 になるタイミングを検出し、データ復号回路 116 において、鍵を更新していけばよい。また、さらに長い周期で更新する場合には、例えば、グループ番号 31 を用いて、トラックアドレス 32 の値が 5 から 0 になる際に、グループ番号 31 を 1 増加させ、0 から 15 の値を繰り返すようにすることで、96 トラックの単位で、しかも C2 パリティの付加の単位の区切り目の、更新のタイミングを検出することが可能となる。

第 18 図は第 13 図の時間情報 25（4 バイト = 32 ビット）の具体

的構成例であり、鍵フラグ、暗号フラグ格納の他の方法を示したものである。ここでは、例えば、時間情報 2 5 1 としては、22 ビットの情報であり、2 5 2 は前述の鍵フラグ（1 ビット）、2 5 3 は、後続の packets データが暗号化されているかどうかを示す暗号フラグ（1 ビット）である。記録時には、第 2 図の入出力制御回路 1 1 9 は、タイムスタンプである時間情報 2 5 1 とともに、暗号フラグ 2 5 3 に、後続の packets データが暗号化されている場合には例えば“1”を、暗号化されていない場合には“0”を格納し、また、鍵フラグ 2 5 2 には、後続の packets データに対応する前述の鍵情報を格納するパケットデータの鍵フラグを格納する。再生時には、第 2 図の入出力制御回路 1 1 9 において、記録時に付加した時間情報 2 5 を取り除いてデータ復号回路 1 1 6 に出力するとともに、暗号フラグ 2 5 3、鍵フラグ 2 5 2 をデータ復号回路 1 1 6 に供給し、データ復号回路 1 1 6 の動作を制御する。

第 19 図は第 2 図のデータ復号回路 1 1 6 の構成図である。1 1 6 1 はパケットデータ入力端子、1 1 6 7 はパケットデータ出力端子、1 1 6 3 a、1 1 6 3 b はデータ鍵入力端子、1 1 6 3 c はデータ鍵選択信号入力端子、1 1 6 3 d は、処理モード選択信号入力端子、1 1 6 2、1 1 6 6 はブロック処理回路、1 1 6 4 は鍵スケジュール回路、1 1 6 5 は復号器、1 1 6 8 a、1 1 6 8 b はデータ鍵レジスタ、1 1 6 9 はデータ鍵セレクタである。データ復号回路 1 1 6 は、あらかじめ定められたデータ鍵により、入力されるパケットデータ単位で復号化して出力する。

復号器 1 1 6 5 は、複数ビットで構成されるブロックを単位として復号処理を実現するブロック暗号を用いる。

25 入力端子 1 1 6 1 から入力されたパケットデータは、データ暗号回路 1 1 5 と同様に、複数ビットからなるブロック C に区切られ、各ブロッ

クは、復号器 1 1 6 5 において順次復号化され、その結果ブロック P を出力し、ブロック処理回路 1 1 6 6 において、パケットデータの形式に戻して出力端子 1 1 6 7 へ出力する。ここで、復号化のための鍵であるデータ鍵は、制御回路 1 0 4 より、データ鍵入力端子 1 1 6 3 a および
5 1 1 6 3 b から入力され、データ鍵レジスタ 1 1 6 8 a、1 1 6 8 b に記憶される。例えば、データ鍵レジスタ 1 1 6 8 a には、現在のデータ鍵を、データ鍵レジスタ 1 1 6 8 b には次に切り換えるデータ鍵を記録させる。

また、処理モード選択信号入力端子 1 1 6 3 d からは、入出力制御回路 1 0 9 より検出した暗号フラグ 2 5 3 が入力され、復号器 1 1 6 5 を復号動作のモードか、何もしないで通過させるモードかを決定する。さらに、データ鍵選択信号入力端子 1 1 6 3 c からは、入出力制御回路 1 0 9 より検出した鍵フラグ 2 5 2 が入力され、データ鍵セクタ 1 1 6 9 により、選択されたデータ鍵が出力される。選択されたデータ鍵は、
15 スケジュール回路 1 1 6 4 においてサブ鍵 K A、K B に変換され、暗号器 1 1 6 5 に供給される。

ここで、第 2 図の入出力制御回路 1 1 9 で検出した、暗号フラグ、あるいは鍵フラグが変化すると、それに連動して、データ復号器 1 1 6 の動作モード、データ鍵の選択が行われる。

20 以上のように、各パケットデータへ暗号フラグ、鍵フラグを付加することにより、パケットデータ単位での、暗号化の有無、鍵情報の判別、および復号処理が実現できる。

その他、暗号化されているかどうかを示す暗号フラグの格納場所としては、第 1 5 図に示した鍵情報を格納するパックの 2 バイト目に格納する方法、あるいは前述の第 1 4 図に示したフォーマット情報 4 5、ブロック情報 4 6 に格納する方法もある。

暗号フラグをフォーマット情報45、あるいはブロック情報46等に格納することで、例えば暗号フラグが“1”を示す時、すなわちパケットデータが暗号化されている場合には、データ復号回路116の動作を復号動作とするとともに、付加情報47の鍵情報を格納するパックから、
5 鍵情報を取得するようにし、暗号フラグが“0”の場合は、データ復号回路116の動作を、復号しないでそのまま出力するようにすることで、パケットデータが暗号化されていない場合の制御動作の簡略化が図れる。また、暗号フラグを鍵情報を格納するパックに格納する方法では、暗号フラグが“0”、すなわちパケットデータが暗号化されていない場合は、
10 そのパックの3バイト目以降のブロック鍵情報は格納されていない。

その他、暗号フラグを用いずに、例えば、鍵情報を格納するパックの有無で暗号化されているかどうかを判別することもできる。

~~第20図は第2図の記録信号処理回路102aおよび再生信号処理回路102bからなるデジタル記録再生信号処理回路102の構成図である。~~
15 400はメモリ回路、401は第2図の制御回路104に従いメモリ回路400を制御するアドレス等を生成するメモリ制御回路、402はC2パリティ演算回路、403はC1パリティ演算回路、404は前記制御回路104からの設定内容に従い記録時のID情報、サブコード生成、フォーマット情報、ブロック情報、鍵情報等の付加情報の付加、
20 および再生時のID情報、サブコード、フォーマット情報、ブロック情報、鍵情報等の付加情報の取得等を行う付加情報処理回路、405は記録時の変調処理及び再生時の復調処理を行う変復調回路である。本実施例では、一例としてC2パリティ演算を行うために6トラックのデータを必要とするため、メモリ回路400は少なくとも6トラック分のデータを蓄積する容量を備えるものとする。
25

記録時には、端子411、413を介して第2図の制御回路104に

より、記録状態に設定される。第2図のデータ暗号回路115で暗号化されたパケットデータが端子410から入力され、メモリ制御回路401の制御信号に従いメモリ回路400に蓄積される。C2パリティ演算に必要なデータが蓄積された後、メモリ回路400から逐次読みだされ、

5 C2パリティ演算回路402に入力されて、所定の演算が行われる。C2パリティ演算回路402で得られた演算結果は、メモリ回路400に蓄積される。一方、端子413を介して第2図の制御回路104からの設定に従い、付加情報処理回路404で、入力された暗号化パケットデータの鍵に対応した鍵情報等のパックデータが生成され、メモリ回路4

10 00に蓄積される。さらに前記した記録ブロックを構成するように、鍵情報等を含めメモリ回路400から読みだされたデータは、C1パリティ演算回路403でC1パリティを付加され、変復調回路405に入力される。変復調回路405で所定の変調処理された信号は、端子414を介して出力され、第2図の記録再生アンプ116、回転ヘッド100

15 を介してテープ111上に記録される。

第21図はデータ記録開始時における信号処理のタイミングを示す図である。第21図(a)はデータ暗号化回路115から入力されるパケットデータ、第21図(b)は、データ暗号化回路115が暗号化の際に用いたデータ鍵、第21図(c)は、前述のC2パリティ43の6トラック単位構成にあわせて、第20図のC2パリティ演算回路402でのC2パリティ演算サイクル(本実施例では6トラック)を示し、第21図(d)は回転ヘッド100を介してテープ111に記録する記録信号を示している。第21図の実施例では、記録開始が設定される時間t1より前にあらかじめブロック鍵Aを生成し、データ鍵Kaを演算して、

25 データ暗号化回路115に供給しておく。また、記録開始が設定される時間t1より前は、記録信号処理回路102aは入力信号に関らずパケ

ット無しとみなして記録信号処理を行うように制御する。これにより、時間 t_0 に記録開始が設定されても、期間 p_0 のデータに対しての C_2 パリティの演算は可能となる。

第2図の制御回路104は、時間 t_0 で記録開始にした時の入力データの C_2 パリティ演算サイクル s_0 が終了して、前記第2の誤り訂正符号を構成する n トラック（本実施例では6トラック）の先頭から記録信号を出力する（第21図（d））ように制御する。また、データ鍵は、この C_2 パリティの演算サイクルで更新される。例えば、時間 t_2 より前にブロック鍵 B を生成し、データ鍵 K_b を演算してデータ暗号化回路115に供給しておき、時間 t_2 の時点でデータ暗号化回路115においてデータ鍵を K_b に切り換える。通常、データ暗号化回路115は、その処理のため、パケットデータの入力から出力までの間に遅延時間が生じる。そこで、時間 t_2 からデータ暗号化回路115がパケットを暗号化処理することにより生じるデータ遅延時間分前の時点で、データ暗号化回路115に供給するデータ鍵を K_b に切り換える。あるいは、データ鍵が切り換えられたパケットデータからは、次の演算サイクルの処理に先送りしてもよい。この実施例では、先頭部分に余分なデータが記録されるが、記録開始にする時間 t_1 のタイミングによらず、記録すべき信号に対し C_2 パリティを付加し、上記 C_2 パリティ演算サイクル単位で記録できる。また、再生時において、先頭の余分なデータ部分は、パケット無しとみなして記録処理しているので、 C_2 パリティ演算に用いられるだけで、出力されることはない。

記録終了時には、前記記録再生信号処理回路102aの、テープ111への記録動作を、複数トラックのデータを用いて演算する C_2 パリティの演算サイクル（本実施例では6トラック）完結で行うように前記制御回路104で制御する。この制御方式により、記録開始、記録終了の

切換えタイミングによらず、テープ 1 1 1 上の記録データに全て C 2 パリティを付加し、C 2 パリティの演算サイクル単位で鍵情報が更新され、
5 パケットデータが暗号化されるので、再生時には、C 2 パリティ演算サイクル単位で再生でき、C 2 パリティ演算が可能となるので、鍵情報のデータ信頼性も向上する。

第 2 2 図は第 2 図のテープ 1 1 1 上の鍵情報を示す図である。同図中、
1 1 1 1 から 1 1 1 7 は、C 2 パリティ演算サイクルである 6 トラック
単位で示した記録トラックである。この図の場合、記録トラック 1 1 1
1 から 1 1 1 3 まだが、ブロック鍵 A、記録トラック 1 1 1 4 から 1 1
10 1 6 まだがブロック鍵 B をもとに暗号化されたパケットデータ、およびそれらに対応した鍵情報であるパケットデータが格納される。また、記録トラック 1 1 1 7 は暗号化されずに記録されたトラックである。この図のように、暗号化されたトラックと、暗号化されていないトラックが同一のテープ上に混在することも可能である。鍵情報の更新は、例えば、
15 4 8 トラック、9 6 トラック等、 $m \times n$ トラック毎（ m は 1 以上の整数、 n は本実施例では 6）、あるいは一つの番組全体等考えられるが、鍵の切り換わり目、あるいは暗号化されたトラックと、暗号化されていないトラックとの境目は、C 2 パリティ演算サイクル（本実施例では 6 トラック）の区切り目である。

20 以上、記録の際の動作について説明した。ここで、鍵情報をサブコード領域（第 9 図の 7）に記録することも可能であるが、鍵情報を、各ブロックのヘッダ（第 1 2 図の 4 4）の部分に格納し、各トラック上のデータ記憶領域（第 9 図の 7）に記録することで、アフレコ等による鍵情報のみの書き換えは困難となる。従って、鍵情報の消失を防ぐことができ、また、故意に鍵情報のみを改ざんして意図的に暗号通信を行うことはできない効果がある。

次に、テープからの再生方法について述べる。

第20図のデジタル記録再生信号処理回路102において、再生時は、端子411、413を介して第2図の制御回路104によって、再生状態に設定される。前記テープ111から回転ヘッド100で再生され、端子414から入力された再生信号は、変復調回路405で復調処理された後、C1パリティ演算回路403でC1パリティ演算を行い、誤り検出およびその訂正を行い、C1パリティ演算結果も一緒にメモリ回路400に蓄積される。C2パリティ演算に必要なデータが蓄積された後、メモリ制御回路401の制御信号に従いメモリ回路400から逐次読みだされ、C2パリティ演算回路402に入力される。C2パリティ演算回路402では、上記データで演算を行い、誤りの検出、訂正処理したデータおよびC2パリティ演算結果を、再びメモリ回路400に蓄積する。

第2図のタイミング生成回路105から端子412を介して入力されるタイミング信号を基準として所定の順番にメモリ回路400からデータを読みだし、前記C1パリティ、C2パリティの演算結果を参照し、誤りの無いデータのみを端子410から第2図の入出力制御回路119に出力する。一方、付加情報処理回路404では、メモリ回路400から読み出したデータから鍵情報やサブコード等を取得し、端子413を介して第2図の制御回路104に送出する。その後、第8図で示した演算、すなわち再生によって得られた鍵情報から、 K_p を取り出し、デバイス鍵発生器117からのデバイス鍵との排他的論理和をとって、ハッシュ関数121の演算を行い、データ鍵を得、第2図のデータ復号回路116に出力する。このデータ鍵は、記録時に用いたデータ鍵と同一のものであり、データ復号回路116において、正しくもとのパケットデータを得ることができる。

第23図は、本発明のデータ再生時における信号処理のタイミングを示す図である。第23図(a)は回転ヘッド100を介してテープ111から再生される再生信号、第23図(b)は上記C2パリティの演算サイクル(本実施例では6トラック)を示し、第23図(c)は入出力制御回路119から出力されるパケットデータを示し、第23図(d)は、第2図のデータ復号回路116に供給されるデータ鍵を示している。付加情報処理回路404では、演算サイクルs3においては、このサイクルで用いられている鍵情報KpCが検出されている。このKpCにより前述の演算で得られたデータ鍵Kcが、例えば前述のデータ鍵レジスタ1163aに記憶されており、データ鍵セクタ1169も、データ鍵レジスタ1163aのデータ鍵Kcが出力されるように選択されている。

次に、演算サイクルs4において、鍵情報KpDが用いられていることが検出されると、あらかじめ、データ鍵Kdを前述の演算で求めておき、データ鍵レジスタ1163bに記憶させ、時間t3のタイミングで、データ鍵セクタ1169を制御してデータ鍵レジスタ1163bのデータ鍵Kdに切り換える。以上の方法により、データ鍵を更新しながらの再生動作が可能となる。

また、既に記録済みのテープに追加記録する場合、C2パリティの付加単位の区切り目から、記録を開始するようにすることで、追加記録直前のトラックの鍵情報のデータ信頼性を損なわずに、つなぎ記録が可能となる。

その他、パケットデータが暗号化されているかいないかを区別する方法としては、第4図で示した同期バイト501は、通常固定データであるので、例えば、再生信号処理回路102bにおいて、この同期バイトの検出を行い、検出できた場合は、第2図のデータ復号回路116を入

力されるパケットデータを何もしないで通過させる機能に切り換え、検出できなかった場合は、第2図のデータ復号回路116を復号機能の動作に切り換え、付加情報エリア内の鍵情報を検出する動作を行うことで、記録時に、パケットデータを暗号化して記録されたトラックと、暗号化
5 しないで記録したトラックとが混在するテープの場合にも、検出が可能となる。

また、あらかじめ記録されているソフトテープについても、以上説明した方法で、ソフトテープの作成および再生が可能となり、テープ上のパケットデータの保護が実現できる。

10 以上は、記録トラックに現在のブロック鍵が格納されている例を示したが、データ鍵の演算は、C2の一演算サイクル内で行わなければならない。C2の一演算サイクル内でデータ鍵の演算が間に合わない場合は、前述のように、記録トラック内に、現在のブロック鍵と、次のブロック鍵を記録しておくことで、あらかじめ、次のデータ鍵を求めておける。

15 第24図は第1図のデジタル信号記録再生装置200の他の構成図である。同図中、121は、例えばIEEE1394のような高速デジタルバスインターフェース等のプロトコルを実現するデジタルインターフェース回路であり、入力されたパケットデータの時間間隔を維持しながら、高速にデータを伝送する機能を有する、122は、デジタル
20 ルインターフェースバスである。123は、デジタルインターフェース122上を伝送されるデジタルデータを保護するための暗号／復号回路であり、パケットデータを暗号化してデジタルインターフェースバス122上に伝送し、あるいは受信したデジタルデータを復号化する。124は、マイクロプロセッサのような制御回路であり、デジタル
25 ルインターフェース回路121、暗号／復号回路123を制御する。

記録時には、デジタルインターフェースバス122上を伝送されて

きた暗号化されたデジタルデータをデジタルインターフェース回路 121において、所定の packets 処理を行い、暗号／復号回路 123において、元の packets データに復号して、入出力回路 107に出力する。その後、前述で説明したように、データ暗号回路 115で packets データを暗号化し、テープ 111上に記録する。再生時には、データ復号回路 116において、再生した packets データを復号化して、入出力回路 107から暗号／復号回路 123に出力し、暗号／復号回路 123において暗号化して、デジタルインターフェース回路 121から、デジタルインターフェースバス 122に出力する。これによれば、テープ上の packets データ、デジタルインターフェースバス上の packets データの双方の保護が実現できる。

なお、以上の実施例では、テープでの記録再生について説明したが、光ディスクや磁気ディスクなどのディスクや、半導体メモリ等、他のあらゆる記録媒体に記録再生する場合でも、同様に適用することができる。

上記ディスクの場合には、鍵情報の切り換え、あるいは暗号化するかしないかの切り換えは、例えばディスクの記録の一つの単位であるセクタの区切り目で行うとよい。

また、上記半導体メモリの場合には、鍵情報の切り換え、あるいは暗号化するかしないかの切り換えは、例えば半導体メモリの記録の一つの単位であるアドレスの区切り目で行うとよい。

また、本実施例は、本発明を、デジタル信号を鍵により暗号化するシステムに適用したものである。しかし、本発明はこの実施例に限定されるものではなく、例えば、デジタル信号がキーコードによりスクランブルされたりするシステムにも適用可能である。すなわち、本発明は、少なくとも、デジタル信号が元々のクリアな状態から変換されるように処理されるあらゆるシステムに対して適用可能なものである。

産業上の利用可能性

本発明によれば、デジタル信号を、記録媒体上に記録または再生するデジタル信号記録装置、再生装置、および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、デジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したデジタル信号を復号化して出力する。以上により、再生の際には、前記所定の演算を施さない限り、前記鍵が得られないので、記録媒体上の鍵情報を得ても、それを用いて暗号化されたデジタル信号を復号することは困難であり、記録媒体上のデジタル信号の著作権を保護することができる。

請 求 の 範 囲

1. デジタル信号を記録媒体上に記録するデジタル信号記録装置において、

- 5 少なくとも一つの鍵情報を発生する鍵情報発生手段と、
前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と前記デジタル信号が入力され、前記鍵で前記デジタル信号を暗号化して出力する暗号変換手段と、

- 10 少なくとも一つの前記鍵情報を、暗号化された前記デジタル信号と共に、前記記録媒体上の所定の領域に記録する記録手段とを
備えたことを特徴とするデジタル信号記録装置。

2. 前記デジタル信号は、所定長のパケット形式を有してなることを特徴とする請求の範囲第1項記載のデジタル信号記録装置。

- 15 3. 前記鍵情報発生手段は、所定時間間隔で少なくとも一つの前記鍵情報を更新していく機能を備え、

前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を、前記記録媒体上の所定の領域に記録する機能を備えたことを特徴とする請求の範囲第1項記載のデジタル信号記録
20 装置。

4. 前記デジタル信号は、所定長のパケット形式を有してなり、

前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を、前記デジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第

- 25 3項記載のデジタル信号記録装置。

5. 前記暗号変換手段は、さらに、前記デジタル信号を暗号化して出

力する機能と、暗号化しないでそのまま出力する機能とを選択できる機能を備え、

前記記録手段は、前記デジタル信号が暗号化されているか否かを示す暗号フラグ情報を前記記録媒体上の所定の領域に記録し、暗号化しない

5 場合は、前記鍵情報を記録しない機能を備えたことを特徴とする請求の範囲第1項記載のデジタル信号記録装置。

6. 前記デジタル信号は、所定長のパケット形式を有してなり、

前記記録手段は、前記デジタル信号が暗号化されているか否かを示す暗号フラグ情報を、前記デジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第5項記載のデジタル信号記録装置。

7. 所定長のパケット形式のデジタル信号を入力して、別の所定長に分割し、同期信号、記録情報信号、付加情報信号、および第1の誤り訂正符号を付加してブロック形式とし、所定数個のブロックを1トラックとし、 n (n は1以上の整数)トラック単位で第2の誤り訂正符号を付加し、前記第2の誤り訂正符号も分割して第1の誤り訂正符号を付加してブロック形式とし、記録媒体上に前記トラックを記録するデジタル信号記録装置において、

少なくとも一つの鍵情報を発生する鍵情報発生手段と、

20 前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と前記デジタル信号が入力され、前記鍵で前記デジタル信号を暗号化して出力する暗号変換手段と、

少なくとも一つの前記鍵情報を、暗号化された前記デジタル信号と共に、前記記録媒体上の所定の領域に記録する記録手段とを備えたことを特徴とするデジタル信号記録装置。

8. 前記記録手段は、前記鍵情報を、前記ブロックの付加情報信号領域に格納して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第7項記載のデジタル信号記録装置。

9. 前記鍵情報発生手段は、所定時間間隔で少なくとも一つの前記鍵情報を更新していく機能を有し、

前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を前記記録媒体上の所定の領域に記録することを特徴とする請求の範囲第7項記載のデジタル信号記録装置。

10. 前記記録手段は、前記タイミングを識別可能な情報を、前記ブロックの記録情報信号領域に格納して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第9項記載のデジタル信号記録装置。

11. 前記記録手段は、前記タイミングを識別可能な情報を、前記ブロックの付加情報信号領域に格納して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第9項記載のデジタル信号記録装置。

15. 12. 前記記録手段は、前記タイミングを識別可能な情報を、前記デジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第9項記載のデジタル信号記録装置。

20. 13. 前記鍵情報発生手段は、前記第2の誤り訂正符号を付加したnトラックの単位の区切り目で、前記鍵情報を更新していく機能を備えたことを特徴とする請求の範囲第9項記載のデジタル信号記録装置。

14. 前記暗号変換手段は、前記デジタル信号を暗号化して出力する機能と、暗号化しないでそのまま出力する機能とを選択できる機能を有し、

25. 前記記録手段は、前記デジタル信号が暗号化されているか否かを示す暗号フラグ情報を前記記録媒体上の所定の領域に記録し、暗号化しない場合は、前記鍵情報を記録しない機能を備えたことを特徴とする請求の

範囲第7項記載のデジタル信号記録装置。

15. 前記記録手段は、前記暗号フラグ情報を、前記ブロックの記録情報信号領域に格納して前記記録媒体上にする機能を備えたことを特徴とする請求の範囲第14項記載のデジタル信号記録装置。

5 16. 前記記録手段は、前記暗号フラグ情報を、前記ブロックの付加情報信号領域に格納して前記記録媒体上にする機能を備えたことを特徴とする請求の範囲第14項記載のデジタル信号記録装置。

17. 前記記録手段は、前記暗号フラグ情報を、前記デジタル信号の各パケットに付加する機能を備えたことを特徴とする請求の範囲第14
10 項記載のデジタル信号記録装置。

18. 前記暗号変換手段は、前記第2の誤り訂正符号を付加した n トラックの単位の区切り目で、前記デジタル信号を暗号化するか否かを切り換える機能を備えたことを特徴とする請求の範囲第14項記載のデ
~~ジタル信号記録装置。~~

15 19. 記録媒体上に記録されているデジタル信号を再生するデジタル信号再生装置において、

前記記録媒体上の所定の領域に記録されている少なくとも一つの鍵情報と、前記デジタル信号とを再生する再生手段と、

前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段
20 と、

前記鍵と再生された前記デジタル信号が入力され、前記鍵で前記デジタル信号を復号化して出力する復号変換手段とを

備えたことを特徴とするデジタル信号再生装置。

20 20. 前記デジタル信号は、所定長のパケット形式を有してなることを特徴とする請求の範囲第19項記載のデジタル信号再生装置。

21. 少なくとも一つの他の鍵情報を発生する、鍵情報発生手段を備え、

前記鍵発生手段は、前記鍵情報と、前記他の鍵情報とが入力されて所定の演算を行って鍵を発生する機能を備えたことを特徴とする請求の範囲第19項記載のデジタル信号再生装置。

22. 前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、更新された前記鍵情報と、前記鍵情報を更新するタイミングを識別可能な情報とを、再生する機能を備え、

前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、所定の演算を行って更新された鍵を発生する機能を備え、

10 前記復号変換手段は、入力された前記鍵を、前記タイミング信号に合わせて前記更新された鍵に切り換える手段を備えたことを特徴とする請求の範囲第19項記載のデジタル信号再生装置。

23. 前記デジタル信号は、所定長のパケット形式を有してなり、

15 前記再生手段は、前記デジタル信号の各パケットに付加して記録されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求の範囲第22項記載のデジタル信号再生装置。

24. 前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、前記デジタル信号が暗号化されているか否か示す暗号フラグ情報を、再生する機能を備え、

20 前記復号変換手段は、前記暗号フラグ情報により、再生された前記デジタル信号を復号化して出力する機能と、復号化しないでそのまま出力する機能とを選択して切り換える機能を備えたことを特徴とする請求の範囲第19項記載のデジタル信号再生装置。

25. 前記デジタル信号は、所定長のパケット形式を有してなり、

25 前記再生手段は、前記デジタル信号の各パケットに付加されて記録されているところの、前記デジタル信号が暗号化されているか否か示

す暗号フラグ情報を、再生する機能を備えたことを特徴とする請求の範囲第24項記載のデジタル信号再生装置。

26. 所定長のパケット形式のデジタル信号を別の所定長に分割し、同期信号、記録情報信号、付加情報信号、および第1の誤り訂正符号を付加してブロック形式とし、所定数個のブロックを1トラックとし、n (nは1以上の整数)トラック単位で第2の誤り訂正符号を付加し、前記第2の誤り訂正符号も分割して第1の誤り訂正符号を付加してブロック形式とし、記録媒体上に記録されている前記デジタル信号を再生するデジタル信号再生装置において、

10 前記記録媒体上の所定の領域に記録されている少なくとも一つの鍵情報と、前記デジタル信号とを再生する再生手段と、

前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

15 前記鍵と再生された前記デジタル信号が入力され、前記鍵で前記デジタル信号を復号化して出力する復号変換手段とを

備えたことを特徴とするデジタル信号再生装置。

27. 少なくとも一つの他の鍵情報を発生する、鍵情報発生手段を備え、

前記鍵発生手段は、前記鍵情報と、前記他の鍵情報とが入力され、所定の演算を行って鍵を発生する機能を備えたことを特徴とする請求の範囲

20 第26項記載のデジタル信号再生装置。

28. 前記再生手段は、前記記録媒体上の前記ブロックの付加情報信号領域に記録されているところの、前記鍵情報を、再生する機能を備えたことを特徴とする請求の範囲第26項記載のデジタル信号再生装置。

25 29. 前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、更新された前記鍵情報と、前記鍵情報を更新するタイミングを識別可能な情報とを、再生する機能を備え、

前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、所定の演算を行って更新された鍵を発生する機能を備え、

前記復号変換手段は、入力された前記鍵を、前記タイミング信号に合わせて前記更新された鍵に切り換える手段を備えたことを特徴とする請求の範囲第26項記載のデジタル信号再生装置。

30. 前記再生手段は、前記ブロックの記録情報信号領域に記録されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求の範囲第29項記載のデジタル信号再生装置。

10 31. 前記再生手段は、前記ブロックの付加情報信号領域に記録されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求の範囲第29項記載のデジタル信号再生装置。

15 32. 前記再生手段は、前記デジタル信号の各パケットに付加されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求の範囲第29項記載のデジタル信号再生装置。

20 33. 前記再生手段は、前記第2の誤り訂正符号を付加したnトラックの単位の区切り目で更新されているところの、前記鍵情報を、再生していく機能を備えたことを特徴とする請求の範囲第29項記載のデジタル信号再生装置。

34. 前記再生手段は、前記記録媒体上の所定の領域に記録されている、前記デジタル信号が暗号化されているか否か示す暗号フラグ情報を再生する機能を備え、

25 前記復号変換手段は、前記暗号フラグ情報により、再生された前記デジタル信号を復号化して出力する機能と、復号化しないでそのまま出

力する機能とを選択して切り換える機能を備えたことを特徴とする請求の範囲第26項記載のデジタル信号再生装置。

35. 前記再生手段は、前記ブロックの記録情報信号領域に記録されているところの、前記デジタル信号が暗号化されているか否か示す暗号
5 フラグ情報を、再生する機能を備えたことを特徴とする請求の範囲第34項記載のデジタル信号再生装置。

36. 前記再生手段は、前記ブロックの付加情報信号領域に記録されているところの、前記デジタル信号が暗号化されているか否か示す暗号
10 フラグ情報を、再生する機能を備えたことを特徴とする請求の範囲第34項記載のデジタル信号再生装置。

37. 前記再生手段は、前記デジタル信号の各パケットに付加して記録されているところの、前記デジタル信号が暗号化されているか否か
~~示す暗号フラグ情報を、再生する機能を備えたことを特徴とする請求の~~
範囲第34項記載のデジタル信号再生装置。

15 38. 前記再生手段は、前記第2の誤り訂正符号を付加したnトラックの単位の区切り目で切り換えられているところの、前記暗号フラグを、再生していく機能を備えたことを特徴とする請求の範囲第34項記載のデジタル信号再生装置。

39. デジタル信号が記録されているデジタル信号記録媒体におい
20 て、

鍵情報に所定の演算を行って得られた鍵で暗号化された前記デジタル信号と共に、前記鍵情報が、所定の領域に記録されていることを特徴とするデジタル信号記録媒体。

40. 前記デジタル信号は、所定長のパケット形式を有してなることを特徴とする請求の範囲第39項記載のデジタル信号記録媒体。
25

41. 前記鍵情報が所定間隔で更新され、所定の領域に記録されている

ことを特徴とする請求の範囲第39項記載のデジタル信号記録媒体。

42. 前記鍵情報が所定間隔で更新されたことを示すタイミングを識別可能な情報が、所定の領域に記録されていることを特徴とする請求の範囲第39項記載のデジタル信号記録媒体。

- 5 43. 前記デジタル信号が暗号化されているか否かを示す暗号フラグ情報が、所定の領域に記録されていて、前記デジタル信号が暗号化されていない場合は、前記鍵情報は記録されていないこと特徴とする請求の範囲第39項記載のデジタル信号記録媒体。

- 10 44. デジタル信号を変換するための複数種類の鍵を発生する鍵発生手段と、

前記鍵を用いてデジタル信号を変換し、変換後の変換デジタル信号を出力する変換手段と、

前記鍵および前記変換デジタル信号を記録媒体に記録する記録手段と、

- 15 を備えてなることを特徴とするデジタル信号記録装置。

45. 複数種類の鍵で変換された変換デジタル信号および前記鍵が記録された媒体が用いられ、

前記変換デジタル信号および前記鍵を前記媒体から再生し、出力する再生手段と、

- 20 前記再生手段からの出力が入力され、前記変換デジタル信号を前記鍵を用いて復号変換する復号変換手段と、

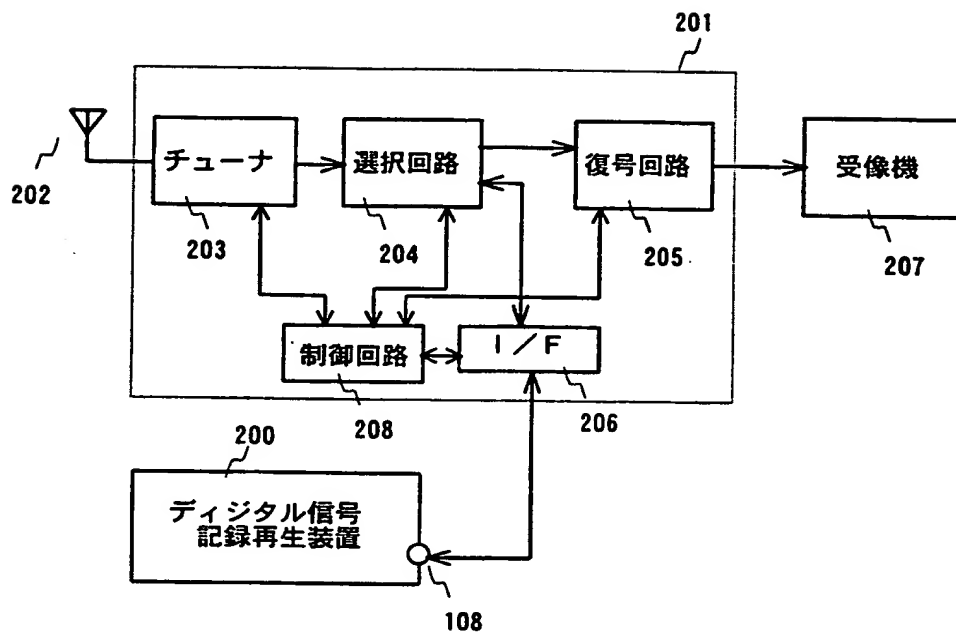
を備えてなるデジタル信号再生装置

46. 複数種類の鍵で変換された変換デジタル信号および前記鍵が記録された記録媒体。

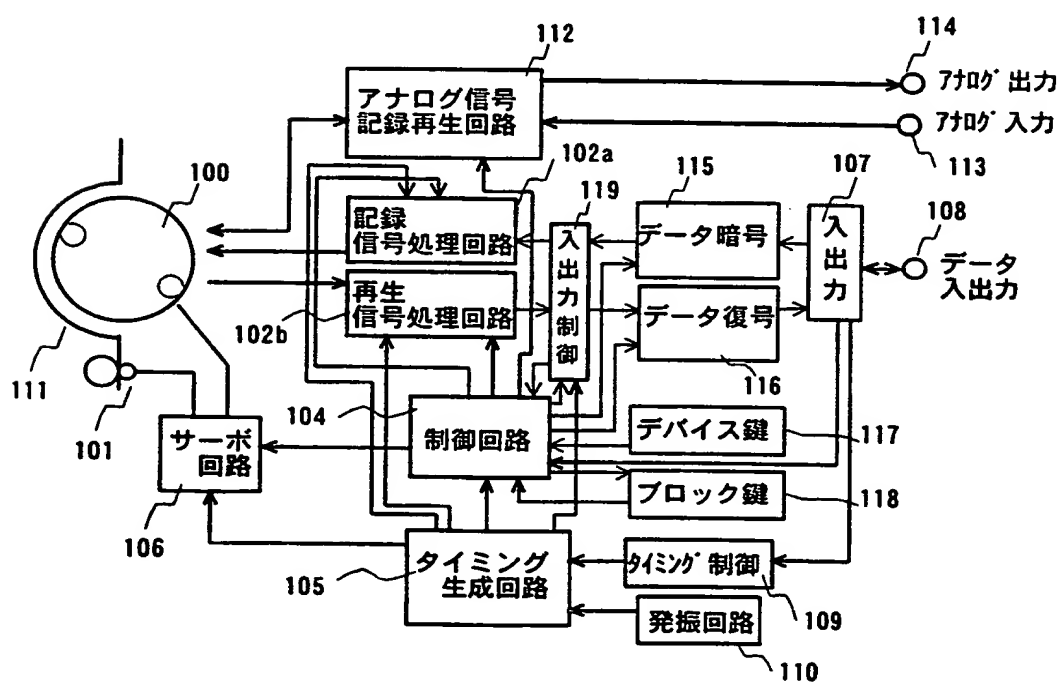
THIS PAGE BLANK (USPTO)

1 / 14

第 1 図



第2図

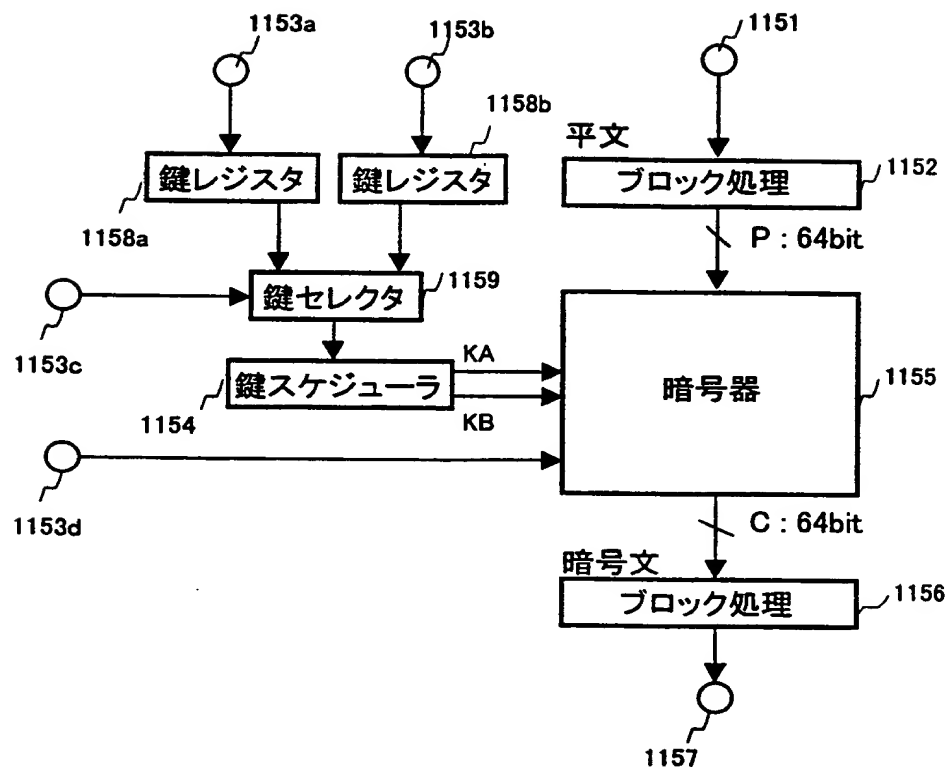


THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

3/14

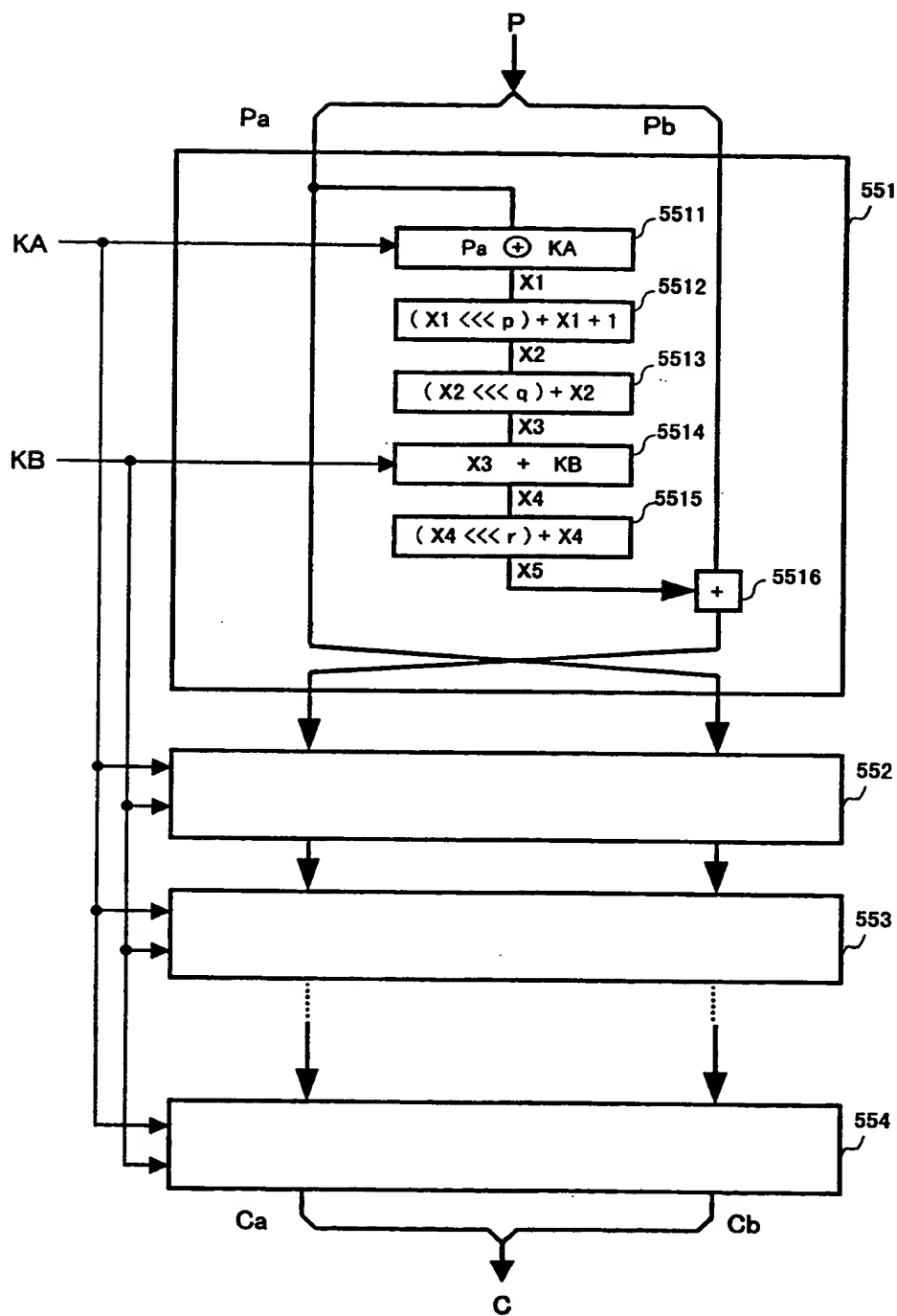
第6図



THIS PAGE BLANK (USPTO)

4/14

第7図

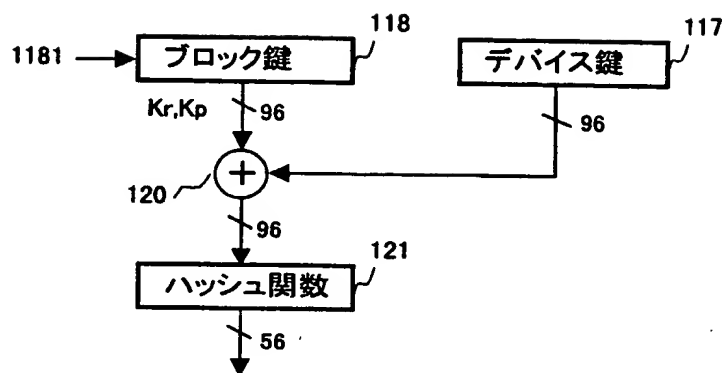


THIS PAGE BLANK (USPTO)

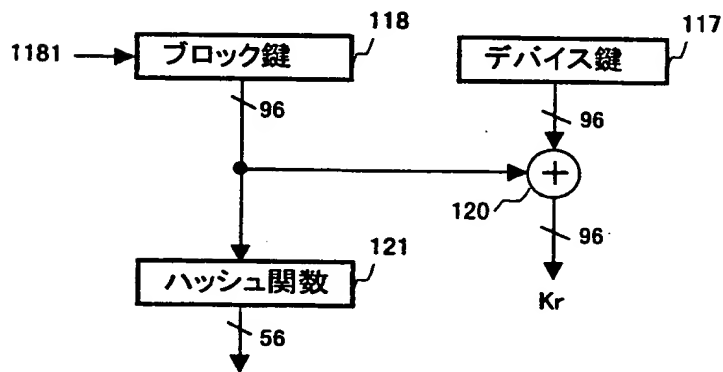
5/14

第8図

(a)



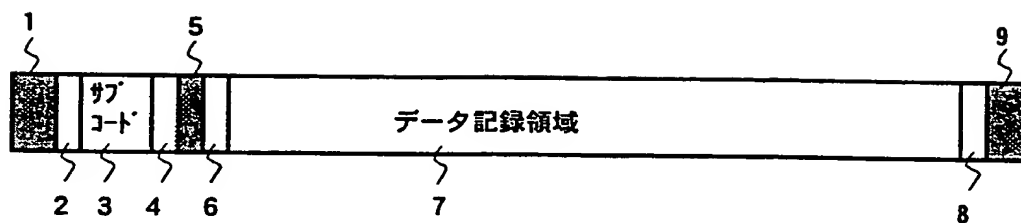
(b)



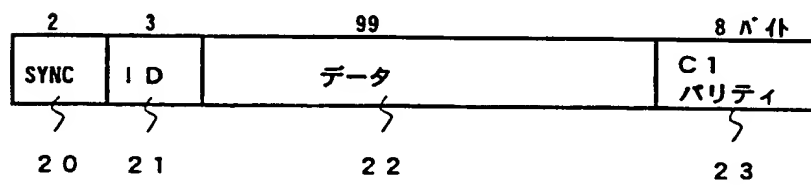
THIS PAGE BLANK (USPTO)

6/14

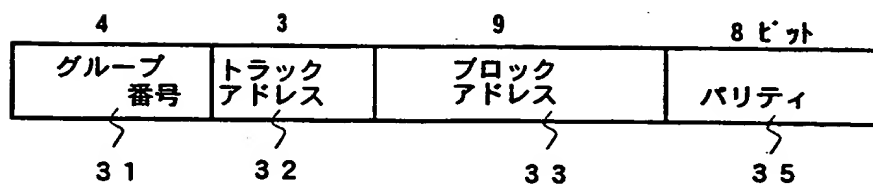
第9図



第10図



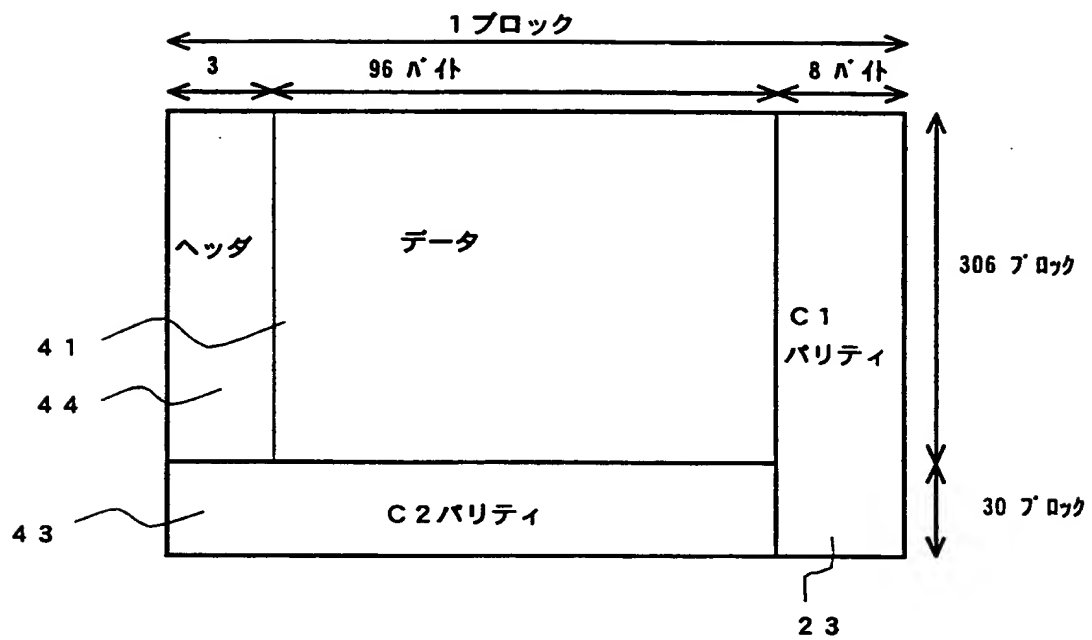
第11図



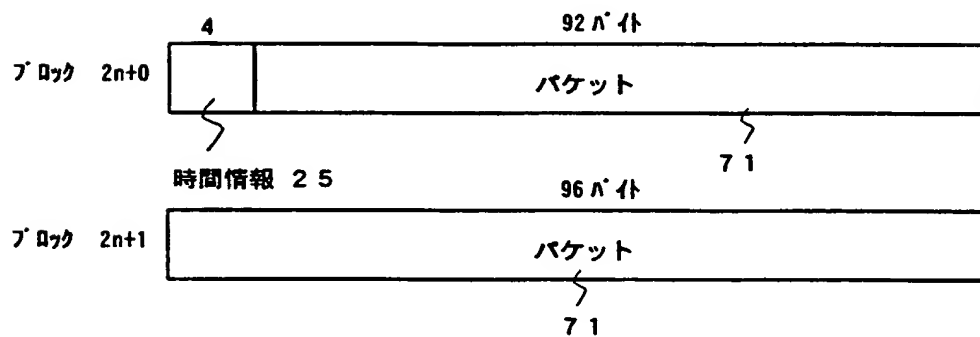
THIS PAGE BLANK (user)

7/14

第12図



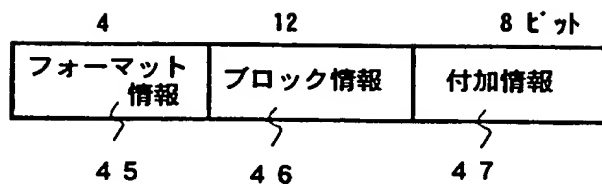
第13図



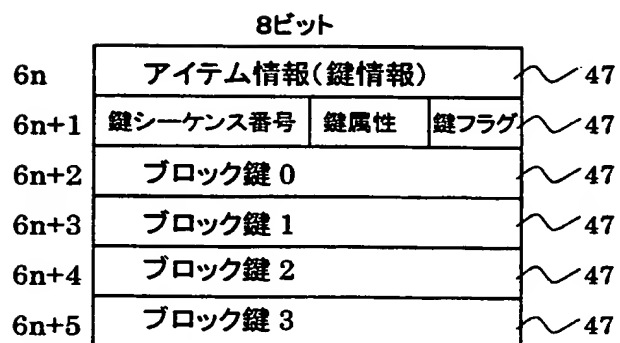
CLARK (USPTO)

8/14

第14図



第15図



THIS PAGE BLANK (USPTO)

第16図

(1)

6a	“鍵情報”		
6a+1	“2”	“0”	“0”
6a+2	ブロック鍵 A0		
6a+3	ブロック鍵 A1		
6a+4	ブロック鍵 A2		
6a+5	ブロック鍵 A3		

6b	“鍵情報”		
6b+1	“1”	“0”	“0”
6b+2	ブロック鍵 A4		
6b+3	ブロック鍵 A5		
6b+4	ブロック鍵 A6		
6b+5	ブロック鍵 A7		

6c	“鍵情報”		
6c+1	“0”	“0”	“0”
6c+2	ブロック鍵 A8		
6c+3	ブロック鍵 A9		
6c+4	ブロック鍵 A10		
6c+5	ブロック鍵 A11		

(2)

6d	“鍵情報”		
6d+1	“2”	“0”	“1”
6d+2	ブロック鍵 B0		
6d+3	ブロック鍵 B1		
6d+4	ブロック鍵 B2		
6d+5	ブロック鍵 B3		

6e	“鍵情報”		
6e+1	“1”	“0”	“1”
6e+2	ブロック鍵 B4		
6e+3	ブロック鍵 B5		
6e+4	ブロック鍵 B6		
6e+5	ブロック鍵 B7		

6f	“鍵情報”		
6f+1	“0”	“0”	“1”
6f+2	ブロック鍵 B8		
6f+3	ブロック鍵 B9		
6f+4	ブロック鍵 B10		
6f+5	ブロック鍵 B11		

THIS PAGE BLANK (USPTO)

10/14

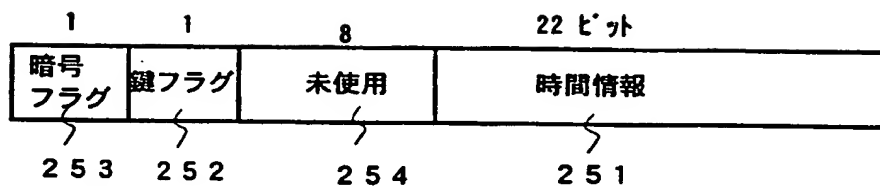
第17図

(1)	6a	“鍵情報”	6b	“鍵情報”	6c	“鍵情報”
	6a+1	“2” “0” “0”	6b+1	“1” “0” “0”	6c+1	“0” “0” “0”
	6a+2	ブロック鍵 A0	6b+2	ブロック鍵 A4	6c+2	ブロック鍵 A8
	6a+3	ブロック鍵 A1	6b+3	ブロック鍵 A5	6c+3	ブロック鍵 A9
	6a+4	ブロック鍵 A2	6b+4	ブロック鍵 A6	6c+4	ブロック鍵 A10
	6a+5	ブロック鍵 A3	6b+5	ブロック鍵 A7	6c+5	ブロック鍵 A11
(2)	6d	“鍵情報”	6e	“鍵情報”	6f	“鍵情報”
	6d+1	“2” “1” “1”	6e+1	“1” “1” “1”	6f+1	“0” “1” “1”
	6d+2	ブロック鍵 B0	6e+2	ブロック鍵 B4	6f+2	ブロック鍵 B8
	6d+3	ブロック鍵 B1	6e+3	ブロック鍵 B5	6f+3	ブロック鍵 B9
	6d+4	ブロック鍵 B2	6e+4	ブロック鍵 B6	6f+4	ブロック鍵 B10
	6d+5	ブロック鍵 B3	6e+5	ブロック鍵 B7	6f+5	ブロック鍵 B11
(3)	6a	“鍵情報”	6b	“鍵情報”	6c	“鍵情報”
	6a+1	“2” “0” “1”	6b+1	“1” “0” “1”	6c+1	“0” “0” “1”
	6a+2	ブロック鍵 B0	6b+2	ブロック鍵 B4	6c+2	ブロック鍵 B8
	6a+3	ブロック鍵 B1	6b+3	ブロック鍵 B5	6c+3	ブロック鍵 B9
	6a+4	ブロック鍵 B2	6b+4	ブロック鍵 B6	6c+4	ブロック鍵 B10
	6a+5	ブロック鍵 B3	6b+5	ブロック鍵 B7	6c+5	ブロック鍵 B11
(4)	6d	“鍵情報”	6e	“鍵情報”	6f	“鍵情報”
	6d+1	“2” “1” “0”	6e+1	“1” “1” “0”	6f+1	“0” “0” “0”
	6d+2	ブロック鍵 C0	6e+2	ブロック鍵 C4	6f+2	ブロック鍵 C8
	6d+3	ブロック鍵 C1	6e+3	ブロック鍵 C5	6f+3	ブロック鍵 C9
	6d+4	ブロック鍵 C2	6e+4	ブロック鍵 C6	6f+4	ブロック鍵 C10
	6d+5	ブロック鍵 C3	6e+5	ブロック鍵 C7	6f+5	ブロック鍵 C11

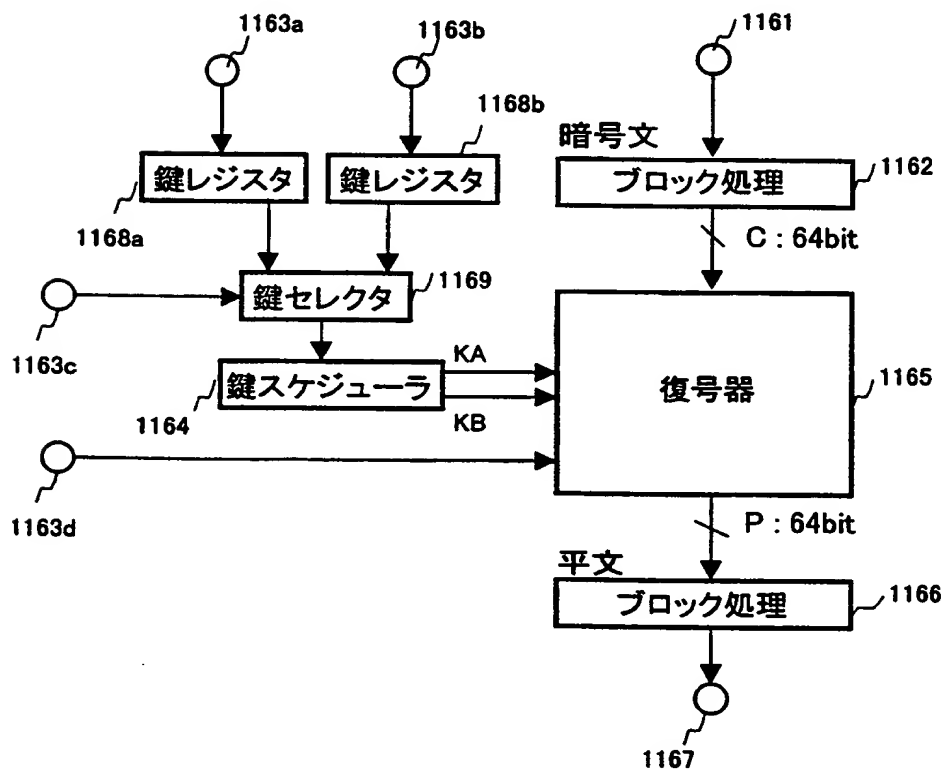
THIS PAGE BLANK (USPTO)

11/14

第18図



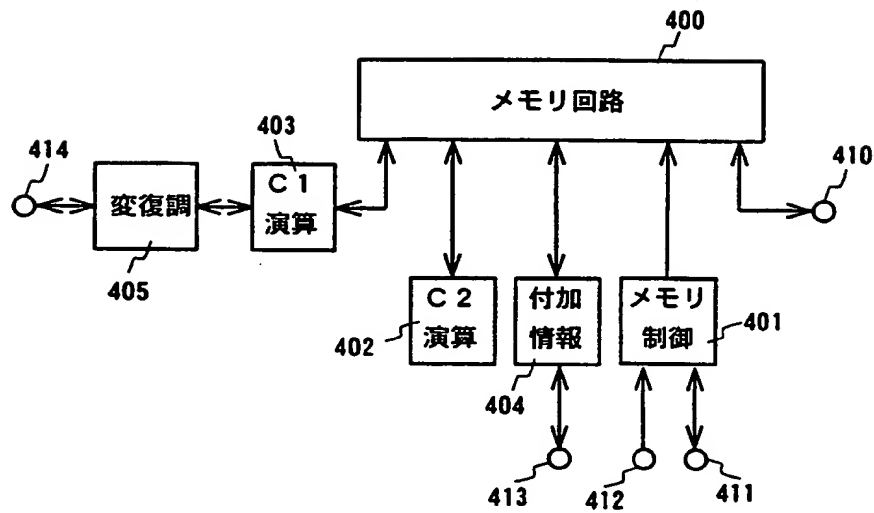
第19図



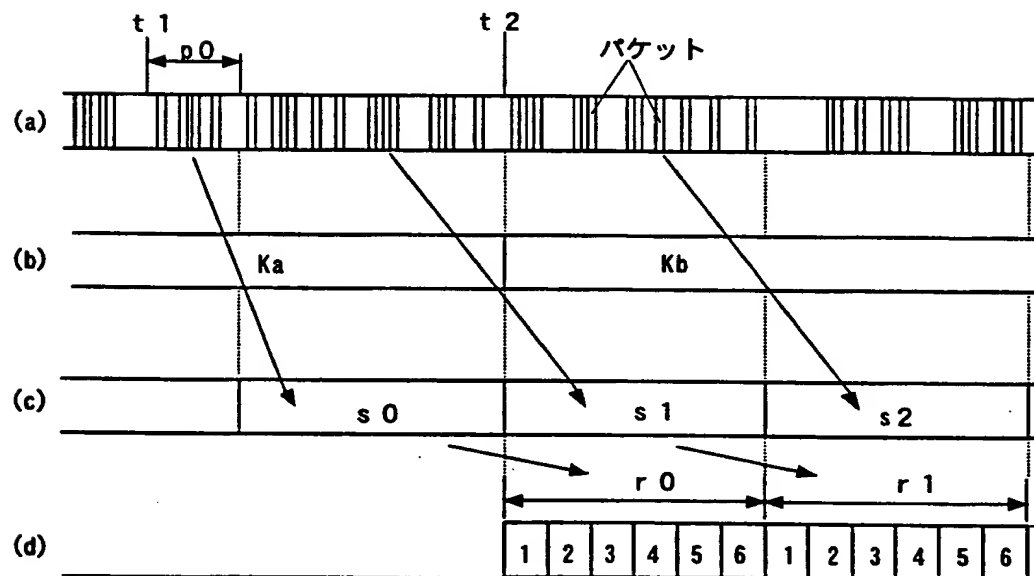
THIS PAGE BLANK (USPTO)

12/14

第20図



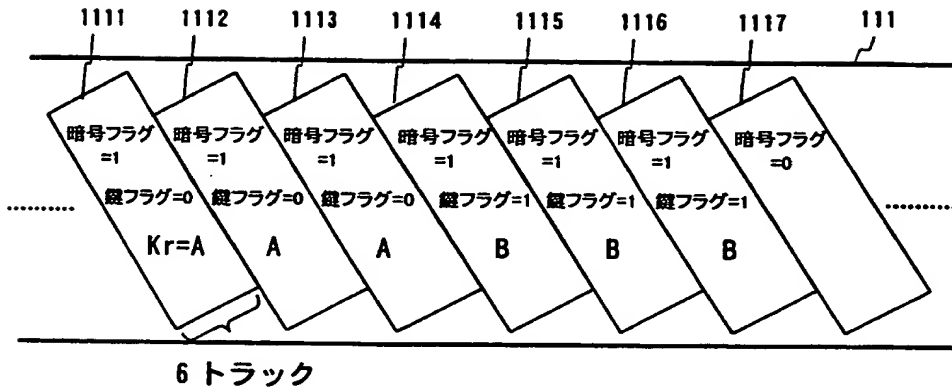
第21図



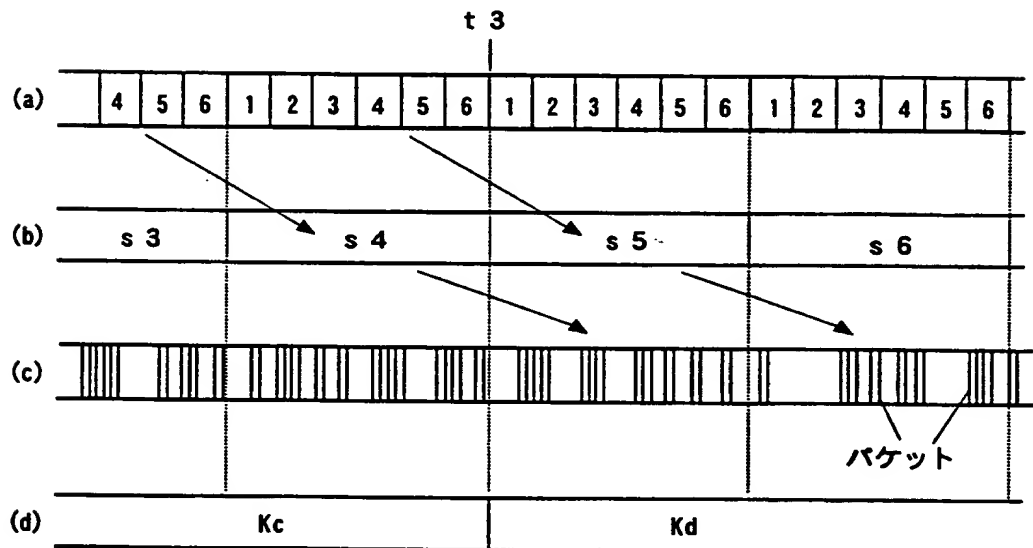
THIS PAGE BLANK (UBFTD)

1 3 / 1 4

第 2 2 図



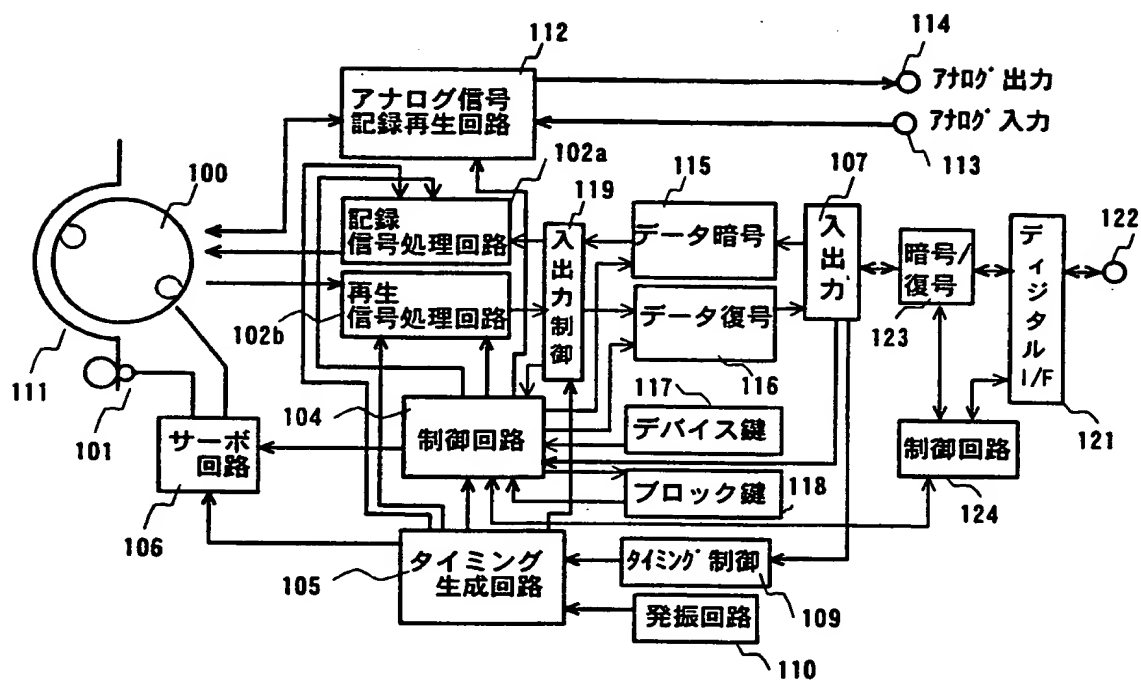
第 2 3 図



THIS PAGE BLANK (USPTO)

14/14

第24図



THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/00929

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁶ G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁶ G11B20/10Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 6-231536, A (Matsushita Electric Industrial Co., Ltd.), 19 August, 1994 (19. 08. 94), Full text ; Figs. 1, 2 (Family: none)	1-46
A	JP, 7-288798, A (Mitsubishi Electric Corp.), 31 October, 1995 (31. 10. 95), Full text ; Figs. 1 to 10 (Family: none)	1-46
A	JP, 9-214882, A (Victor Co. of Japan, Ltd.), 15 August, 1997 (15. 08. 97), Full text ; Figs. 1 to 5 (Family: none)	1-46
A	JP, 10-241287, A (Matsushita Electric Industrial Co., Ltd.), 11 September, 1998 (11. 09. 98), Full text ; Figs. 1 to 9 (Family: none)	1-46

☐ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
---	--

Date of the actual completion of the international search
24 May, 1999 (24. 05. 99)Date of mailing of the international search report
1 June, 1999 (01. 06. 99)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

THIS PAGE BLANK (uspro)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁸ G11B20/10

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁸ G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-1999年
 日本国登録実用新案公報 1994-1999年
 日本国実用新案登録公報 1996-1999年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P, 6-231536, A (松下電器産業株式会社) 19. 8月. 1994 (19. 08. 94) 全文, 第1-2図 (ファミリーなし)	1-46
A	J P, 7-288798, A (三菱電機株式会社) 31. 10月. 1995 (31. 10. 95) 全文, 第1-10図 (ファミリーなし)	1-46
A	J P, 9-214882, A (日本ビクター株式会社) 15. 8月. 1997 (15. 08. 97) 全文, 第1-5図 (ファミリーなし)	1-46

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

24. 05. 99

国際調査報告の発送日

01.06.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

小松 正

5Q

7736

電話番号 03-3581-1101 内線 6922

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 10-241287, A (松下電器産業株式会社) 11. 9月. 1998 (11. 09. 98) 全文, 第1-9図 (ファミリーなし)	1-46